שם המסמך: מודל ההפעלה בענן – פן טכנולוגי		
פרק ראשי: טכנולוגיות	מספר הנחיה: 4.2.9	
פרק משני: מחשוב ענן - CCoE	מס' גרסה: 1.0	בתוקף מ- 01.12.2022

1. מטרת המסמך

מסמך זה עוסק בפן הטכנולוגי של מודל ההפעלה בענן הממשלתי. מטרת המסמך היא לפרט את יסודות טכנולוגיית הענן ועקרונות הפעולה ליישום מיטבי של ענן בממשלה בהיבטים הטכנולוגיים. מסמך זה הוא חלק מתפיסת הפעלה הוליסטית, אשר חלקיה הנוספים יעסקו בהיבטים הארגוניים של מודל ההפעלה – תהליכים ואנשים.

2. קהל היעד

- מנהלי אגפי הטד"מ (טכנולוגיות דיגיטליות ומידע) במשרדי הממשלה וביחידות הסמך
- מנהלים טכנולוגיים במשרדי הממשלה (CTO)
- ארכיטקטים ומובילי ענן במשרדי הממשלה
- יחידות המטה השותפות אסטרטגיית הענן: מנהל הרכש, מערך הסייבר הלאומי, אגף התכנון במשרד רוה"מ, אגף התקציבים במשרד האוצר, החשכ"ל, ועוד.
- יחידות מטה במשרדי הממשלה העוסקות במעבר לענן
- צוותי מערך הדיגיטל הלאומי העוסקים ביישום מערכות בענן

3. רקע

פרק זה מתאר את מודל הפעלת הענן של ענני נימבוס.

המושג "מודל הפעלה בענן" מתאר את האופן שבו אנשים, תהליכים וטכנולוגיה עובדים יחד בסביבת ענן באופן סינרגטי כך שמובטחת מהירות במתן מענה טכנולוגי מיטבי עבור צורך עסקי תוך שימוש ביכולות ענניות חדשניות ומתקדמות.

האיור להלן מציג את שלושת המרכיבים העיקריים של מודל הפעלת הענן והרכיבים הכלולים בהם: אנשים, טכנולוגיה ותהליכים.

יעדי מודל ההפעלה בענן

מודל ההפעלה בענן נגזר מתוך תפיסת ההפעלה לענן בממשלה אשר מתוארת במסמך האסטרטגיה הממשלתית לענן.

בעת המעבר לענן יש לייצר מודל הפעלה מיטבי המשתלב עם מטרות אסטרטגיית ענן הממשלתית ויעדיה:

- שיפור השירותים והמוצרים הדיגיטליים לציבור
- ביצוע קפיצת מדרגה ביכולותיה הטכנולוגיות של הממשלה
- שיפור האפקטיביות וייעול ההוצאה הממשלתית בתחום הטכנולוגיה
- חיזוק היכולות המקצועיות של הממשלה
- הבטחת המשילות, הריבונות וההגנה בסייבר על התשתיות הטכנולוגיות והמידע הממשלתי בענן

מודל ההפעלה המפורט במסמך זה יספק לממשלה מספר יתרונות מרכזיים בנושאי התכנון, ההטמעה והתחזוקה של מערכות מחשוב ושירותים דיגיטליים:

- **פריסת מערכות מהירה**: בזכות הסינרגיה בין אנשים, תהליכים וטכנולוגיה, מערכות מבוססות ענן יכולות לעלות במהירות לאוויר, בהתאם לדרישות העסקיות של לקוחות המערכת. מודל ההפעלה בענן מאפשר מעבר חלק מתשתית סטטית/קשיחה לסביבה דינמית/מודולרית – כזו המאפשרת גמישות רבה יותר.
- **יכולת גידול פשוטה:** הענן מבטל את התלות בין המערכות הפיזיות המותקנות במשרד עצמו (on-premise), על המגבלות הקשורות בשדרוגן, ובין יכולת הגידול שלהן לטובת התאמה לדרישות נוספות. הענן מאפשר תוספת משאבים ללא התחשבות בצורך לרכוש ולהתקין חומרה נוספת.
- **אימוץ מואץ של טכנולוגיות:** הגירה של מערכות לענן מאפשרת אימוץ מהיר יותר של טכנולוגיות חדשות, באופן אפקטיבי מבחינת עלות-תועלת (cost-effective), ובזמן הנדרש (just-in-time), וזאת, בתגובה להתפתחות בצרכים המשתנים בין המשרדים והיחידות ובדרישות המגוונות.
- **מודל ברור של שקיפות ואחריות:** מאפשר מבט אחוד על מחזור החיים של הרכיבים השונים הפועלים בענן. מאפשר ניטור ובקרה של היבטים שונים כדוגמת ביצועים, צריכת משאבים, תקלות וכדומה – כל זאת באופן פשוט וברור.
- **יעילות וגמישות ארגונית:** מודל ההפעלה בענן מאפשר תיאום בין גורמים לצורך זיהוי חוסר יעילות בניצול משאבים כתוצאה מחוסר יעילות תהליכית, על ידי איזון משאבים. איזון זה מבטיח לא רק ניצול אפקטיבי יותר של משאבי המחשוב אלא מבטיח תגובתיות טובה יותר לשינויים ארגוניים.
- **הבטחת התייעלות פיננסית (cost-effectiveness):** הענן מביא אתו מודלים שונים של תשלום, כאשר pay-as-you-go הוא למעשה המודל הנפוץ והשגור ביותר בתעשייה. מודל זה מאפשר תשלום רק לפי הצורך, במקום להוסיף קיבולות למערכות מקומיות על בסיס מודלים שונים של ניבוי וגידול, שאין בהם ודאות.
- **בקרה משופרת**: מודל ההפעלה בענן שם דגש על העמידה בדרישות רגולציה עדכנית, נהלים, סטנדרטים ופרוטוקולים, באופן שמאפשר ואף מחייב שקיפות בין ספקיות הענן לממשלה, בין אם בהבטחת עמידות המערכות הפועלות בענן תחת האילוצים וההנחיות שנקבעו ובין אם בהגדרת הדרישות.
- **אבטחת מידע**: ספקיות הענן שמות דגש רב ומשקיעות משאבים לא מבוטלים בהבטחת העמידה של סביבות הענן שלהן בתקנים המקובלים בתעשייה ובדרישות ותקנות הממשלה כפי שהוגדרו. הן מטמיעות את הכלים והפתרונות הטובים בתחום, מיישמות מדיניות (policies) ו- best practices, אשר מתעדכנים באופן קבוע ומתאימות את עצמן גם לגידול הנדרש.

מימוש יתרונות אלו מתאפשר כתוצאה משימוש בטכנולוגיות מתקדמות אשר מתפתחות באופן מהיר כפועל יוצא מהשקעות ענק שמבצעות ספקיות הענן. קצב התקדמות הפיתוחים והטכנולוגיות החדשות מניע את עולם הענן בקצב מהיר מכפי שהורגלנו אליו בעבר. כדי לנצל את היתרונות הגלומים בטכנולוגיות הענן, תוך שמירה על COST-EFFECTIVENESS, על אבטחת מידע והבטחת עמידה בתקני מדיניות אבטחה בענן (CLOUD POLICIES), הקפדה על הפרוטוקולים והסטנדרטים הנובעים ממדיניות אחידה של הממשלה החלה על כלל המשרדים, יש להבטיח את השיתופיות, ולשמר רמת בקרה ומשילות גבוהה, לצד מקסום השימוש בתשתיות משותפות, ומשאבים משותפים.

4. מבוא לפן הטכנולוגי

פרק זה מפרט את הרקע, מושגי היסוד ורכיבי טכנולוגיית ענן, כבסיס לתפיסת ההפעלה הטכנולוגית שפותחה בממשלה.

4.1. **איזור נחיתה**

איזור נחיתה ארגוני בענן (Landing Zone)

- "איזור נחיתה" הוא תצורת הליבה הבסיסית של כל סביבת ענן. אזורי נחיתה מספקים סביבה מוגדרת מראש - המוקמת בקוד - עבור ספקי ענן שונים כגון Google Cloud ו- AWS.
- "אזור נחיתה" הוא "סביבה מוגדרת עם מערך סטנדרטי של תשתית ענן מאובטחת, כללי מדיניות, שיטות עבודה מומלצות, הנחיות ושירותים מנוהלים באופן מרכזי" תחת חשבון ראשי אחד (Root). הארגון, כלומר "החשבון הראשי", יוצר ואוכף מספר היבטים בנקודת בסיס עבור "היחידות הארגוניות": מדיניות אבטחה, עבודה ברשת, קטלוג שירותים, שירותים משותפים בענן, מאגרי תבניות, ואמצעי ניטור והגנה. הארגון (החשבון הראשי) פועל כ"מנהל-על של הענן" הוא יכול לתת הרשאות לכל תת-גורם לפעול באופן עצמאי בהתאם למדיניות שהוגדרה, כך שמנהל-העל מחיל כללי מדיניות ומוודא שהענן ומהנדסי הפתרונות מגדירים את תצורת שירותי הענן ומשתמשים בהם בהתאם לכללים שהוגדרו מראש. מערך היררכי זה של מבנה החשבונות, הכולל ערכה יחידה של כללי מדיניות והנחיות המוחלים על השימוש בענן, הוא חלק ממהות המודל של עבודה ב-"אזור נחיתה".
- אזורי נחיתה הם מבנה שיש בו תפיסה קונספטואלית אחידה בין ספקי הענן הכולל שירותים משותפים וחשבונות של ארגוני-משנה בכל אחד מספקי הענן, אשר מאפשרים לממש את אמצעי ההגנה הארגוניים ולהקצות שירותים משותפים ולעדכן "מדיניות-על" (Policy).

4.2. **חשבון ענן**

- המושג חשבון ענן מתאר הרשאת גישה עם זיהוי (username/password) ייחודי המוקצה למשתמש, אשר הכרחי לשימוש במוצרי הענן, ומשמש למטרות ניהול וחיוב הקשורות למשאבי ענן, אחד או יותר. לכל חשבון ענן יש כתובת לחיוב (Billing) עבור משאבים המשוייכים אליו, ובגין פעילות המתבצעת באמצעותם.

4.3. **משאבי ענן**

- משאב ענן (Cloud Resource) יכול להיות אחד משלושת ההגדרות מטה :
- מכונות וירטואליות (VM) עם יכולות חישוב ואחסון ספציפיות הניתנות ללקוחות הענן בצורה של מופעי ענן. לקוחות ענן יכולים לשכור מופעים אלה בהתאם לזמינותם ולמנגנון התמחור המיושם.
- מודול המאפשר גישה למאגר משותף של משאבי מחשוב הניתנים להגדרה (למשל, רשתות, שרתים, אחסון, יישומים ושירותי רשת שונים). גישה זו זמינה בכל מקום, לפי דרישה.

- שירות או משאב פיזי או וירטואלי של ספק הענן הנגיש ללקוחות הענן.

4.4. ענן פרטי וירטואלי (VPC)

- ענן פרטי וירטואלי (VIRTUAL PRIVATE CLOUD – או בקיצור VPC) הוא למעשה יחידת החלוקה הלוגית של ארכיטקטורת הענן הציבורי של ספק שירותי ענן (CLOUD SERVICE PROVIDER – CSP). מודל זה מאפשר לארגון להשיג את היתרונות של ניהול "פרטי" של משאבים כאילו היה מדובר בענן פרטי ממש - כמו שליטה מפורטת יותר ברשתות וירטואליות וסביבה מבודדת לצורך הקמת והפעלת שרתים ואפליקציות (WORKLOAD) - תוך ניצול משאבי הענן הציבורי.
- משאבי ענן ציבורי במסגרת חשבונות ענן ציבורי מאוגדים לעננים פרטיים וירטואליים. דבר זה דומה במידה מסויימת לסגמנט רשת פיזית נפרדת של שרתים במסגרת DATA CENTER פיזי בחצרי הממשלה (ON-PREM), אלא שכאן מקושרים ל-VPC משאבי ענן שאינם בהכרח מחשבים. ניתן לייצר קשר בין עננים וירטואליים פרטיים שכאלה באמצעות הגדרות של קישוריות ורכיבי תקשורת וירטואליים, אפילו אם הם שייכים לחשבונות ענן שונים ונפרדים.

במסגרת כל אחד מה-VPC-ים קיימות הגדרות לסגמנטים וירטואליים של רשתות המקשרות שרתים (IaaS) ושירותים (PAAS). תחת זה ניתן להגדיר עוד תתי-רשתות (SUBNETS) בדומה לאופן שבו מגדירים זאת ברשתות וירטואליות במרכזי המחשוב בחצרי הממשלה (ON-PREM).

4.5. ניהול זהויות ובקרת גישה (Identity & Access Management Solution)

- מערכת לניהול הרשאות, משתמשים וזהויות מאפשרת יכולת ניהול מרכזית פשוטה ובהירה של כלל הזהויות השונות של משתמשים במערכות הענן, בקרת הזדהות וניהול הרשאות גם תוך ריבוי עננים ותשתיות שחלקן ON-PREM ("ענן היברידי") ומספקת יכולות בקרה ומעקב אחר הפעילויות השונות במערכת. מערכות אלו מנהלות את כל מחזור החיים של המשתמשים במערכת (הגדרה, בקרה, מתן הרשאות, מעקב שימוש, השעייה, ביטול וכו').
- מנהלת מערך של הגדרות ותקנים אשר מספקים עקרונות לניהול חכם של משתמשים במערכות ענן, מערך ההגדרות מאפשר לזהות באופן ברור את סוג הזהויות וההרשאות שיש להעניק לכל משתמש במערכות השונות של הארגון לצד יכולת לזהות את המשאבים לו כל משתמש צריך גישה על מנת לספק יכולת ניהול איכותית, המערכת מאפשרת לארגון לעמוד בסטנדרטים הבין לאומיים של הרשאות ובקרת גישה באופן פשוט וברור.

4.6. כלי ניטור והתרעה (Alerting and Monitoring Tool)

- כלים לאיסוף כלל הלוגים, לניטור ובקרה שיאפשרו להציג תמונת מצב נוכחית ועדכנית של חשבון הענן, תשתיות ומערכות, אבטחת מידע ואירועי שימוש במערכת וסייבר (אירועים שגרתיים ואירועים חריגים), לרבות מידע המשמש לחיוב בגין שימוש במשאבים.
- הלוגים והניטור חלים גם על כל שינוי תצורה או הוספת רכיב, קישור רשת, חוק ניתן ב/סינון, וכו' המתבצעת בחשבון

4.7. ניהול שירותי IT (IT Service Management – ITSM)

- כלי ITSM הם כלים המספקים לרוב פורטל ניהולי לטיפול בבקשות שירות ופניות משתמשים, מעקב אחר הפניות והטיפול בהם, ובמסגרתם מוטמעת אוטומציה של פעולות שירות שונות הקשורות לתפעול הענן ומשאביו. פלטפורמת ITSM מאפשרת הטמעה וניהול של שירותים דיגיטליים באופן איכותי ובטוח יותר, תוך בקרה של רמת השירות, ניהול ומעקב של עמידה ב- SLA וסטנדרטיזציה של תהליכים המתבצעים באגפי טכנולוגיה דיגיטלית ומידע (טד"מ) בכלל משרדי הממשלה.
- כלים אלו תומכים באינטגרציה עם:

- תהליכי אוטומציה של פעולות תפעול ענן שונות (Cloud Operation / Automation)
- תהליכי ניהול, גילוי ובקרת הקונפיגורציה של השירותים (Change + Service Discovery Management + CMDB)
- תהליכי ניהול בקרת חיוב (Billing Management)
- ניהול אירועים (Incident Management)- לרוב מודול של ITSM
- ניהול קטלוג שירותים מאושרים לשימוש (Service Catalogue Management), - לרוב מודול של ITSM
- ניהול ידע / שאלות ותשובות של משתמשים לבעיות נפוצות (Knowledge Management) – לפעמים ממומש כמודול של ITSM ולפעמים באינטגרציה לכלי חיצוני
- תהליכי טיפול בבקשות משתמשים (Request Management) – לרוב מודול של ITSM
- דוחות בקרה אופיניים לכל תהליכי השירות הנ"ל (לפי תקן ITIL).

- בעידן הענן קיים הצורך בשילוב של כלי ITSM במסגרת פלטפורמות ארגוניות לניהול ענן, מצד אחד בשל המורכבות הגוברת של הפתרונות והוירטואליות של הרכיבים והמערכות, ומצד שני כדי למקסם את יתרונות הענן בתחום האוטומציה של תהליכי ניהול באופן מאובטח יותר, תוך הקטנת טעויות משתמש וסטנדרטיזציה של תהליכים ומושגים בעולם ניהול השירות למשתמשים, על סוגיהם השונים.

4.8. רכיבי תשתית תקשורת בענן (Cloud Networking Components)

רשת ענן מורכבת ממגוון רכיבים וירטואליים המייצגים רכיבי חומרה פיזיים שונים אשר ניתן למקם במספר מיקומים גיאוגרפיים (REGIONS ו-"אזורי זמינות" שהם למעשה חוות שרתים הממוקמות במתקני מחשב נפרדים). החומרה כוללת ציוד רשת, כמו מתגים, נתבים, חומות אש ומאזני עומסים, מערכי אחסון, התקני גיבוי ושרתים. רכיבי תשתית התקשורת מותקנים למעשה כ- VIRTUAL APPLIANCES (בלומר מכונות ושירותים וירטואליים במודל PAAS או IAAS) הנגישים בענן, רבים מהם מסופקים ע"י ספקי הענן ואחרים מסופקים ע"י ספקי צד ג' בענן. קיים גם מודל בו רכיבי תקשורת זמינים כ- SAAS.

4.9. רכיבי אבטחת מידע בענן (Cloud Security Components)

כלים ותשתיות שנועדו ליצירת ארכיטקטורה מאובטחת זמינים בענן (בדומה לרכיבי תקשורת). הכלים מבצעים בקרה אחר הפעילות השוטפת לאיתור כשלים ובעיות קונפיגורציה. זמינותם בענן מאפשרות אכיפת מדיניות טכנולוגית, הכתבה של תאימות לסטנדרטים וכללים שהוגדרו, בדיקת תאימות לסטנדרטים אלו ונאותות רמת אבטחה של פתרונות ומערכות, כלים לניטור הרשת ושילוב פרוטוקולי אימות אמינים. הקצאת רכיבי אבטחת המידע והתצורה שלהם מנוהלת באמצעות מסכי מנהל מערכת ו/או שימוש בקבצי קונפיגורציה ובממשק תכנות API עבור קבצי "סקריפט" של קוד הקמה וקונפיגורציה של תשתיות (INFRASTRUCTURE AS CODE – IAC).

4.10. מימוש מדיניות אבטחת מידע בענן (Policy)

אלמנט חשוב של אבטחת מידע בענן הינו קבצי מדיניות אבטחת מידע טכנית/טכנולוגית בענן (POLICY AS CODE) המהווים מימוש טכנולוגי של המדיניות באמצעות קוד, אשר מכילים למעשה הגדרות תצורה קריטיות לכל רכיב ורכיב, פרוטוקולים, הגדרת בדיקות תאימות ונאותות, הגדרות/אפשרויות גישה ובררות מחדל שונות ועוד כהנה וכהנה הגדרות שונות, אשר ניתן לנהל בקבצים או קוד באופן מרכזי, לתחזק גרסאות ולהפיצם לכל הרכיבים במערכת אשר אליהם ההגדרות רלוונטיות אליהם. ניהול מדיניות אבטחת מידע טכנית (POLICY) באמצעות קבצים אלו (POLICY AS CODE) מאפשר לאכוף את מדיניות אבטחת המידע באופן טכני ממש ברכיבים השונים, לעקוב ולנהל שינויים וגרסאות שלה כפי שמנהלים גרסאות במערכות ניהול קוד, קבצים וקונפיגורציה של תוכנה, לעדכן קונפיגורציה בהתאם לצורך, להפיץ להתקין ולבדוק שינויים כאלו בין סביבות כפי שנעשה בתהליכי פיתוח ואינטגרציה מודרניים

של תוכנה (DevOps – CI/CD Code Pipelines). תהליך זה נקרא Policy Lifecycle ובדומה לתוכנה – דורש התאמות ובקרת קונפיגורציה לפני כל שילוב גרסה חדשה.

5. עקרונות ההפעלה

לאחר העמקה במושגי היסוד בפרק הקודם, מבוא לפרק הטכנולוגי, פרק זה מפרט את עקרונות ההפעלה ליישום טכנולוגי שיוביל למימוש יתרונות הענן באופן המיטבי.

5.1. עקרונות מנחים לארכיטקטורה ומימוש טכנולוגי של מודל ההפעלה הממשלתית בענן:

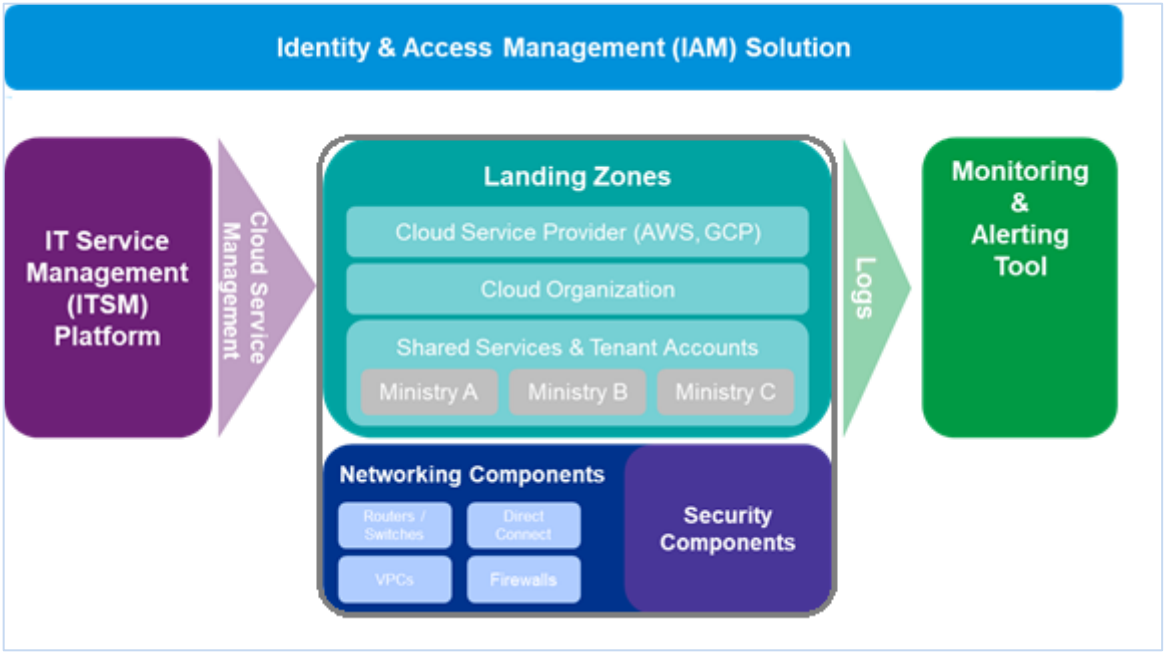
- פרויקט נימבוס מוגדר למידע בלמ"ס.
- תפיסה אחודה של עבודה בענן במסגרת פלטפורמה לניהול תשתיות מחשוב בענן, הבנויה מסביב לאיזור נחיתה, היא הבסיס להקמת מערכות והעברתן מחצרי הממשלה לענן.
- עצמאות משרדית מלאה בכל הנוגע לתפעול החשבון המשרדי בענן.
- פיתוח ותחזוקה מרכזית של תשתיות ושירותים משותפים במטרה להרוויח יתרונות הגודל, לחסוך עלויות ולאפשר שיתופיות בין משרדי הממשלה.
- קידום פתרונות טכנולוגים שיתרמו לקידום תרבות של שיתוף ארגוני בין משרדי הממשלה – שיתוף מידע, שיתוף של שירותים, שיתוף מאגרים , שיתוף פתרונות, קוד תוכנה, ידע, פרוייקטים משותפים למספר משרדים במטרה לחסוך עלויות ולאפשר אחידות ובדומה.
- הטמעת פתרונות טכנולוגיים, כלים, שיטות עבודה מומלצות (Best Practices) ומתודולוגיות, שיאפשרו קיצור מחזורי פיתוח ותחזוקה (Time To Market), זריזות/גמישות (Agility) ותגובתיות גבוהה לדרישות העסקיות המשתנות של הממשלה.
- בניית ארכיטקטורה כלל-ממשלתית בענן, שתקדם שילוב מערכות כולל, ברוח תפיסת Ask Once; שילוב מערכות מונחה אירועים ופרואקטיבי ("ממשלה יוזמת"), סביב מחזור חיי המידע, כשהאזרח והאירועים בחייו הם במוקד, ומחוללים את זרימת המידע בין המערכות.
- מימוש תשתיות מערכות המידע בענן תוך שימוש באוטומציות ובקוד (Infrastructure as Code).
- הגדרות תקני מדיניות ממשל ענן, דרישות הגנת סייבר ואבטחת מידע אחידה ברמה כלל-ממשלתית (Policy as Document) תוך שיתוף מדיניות בקוד תוכנה בין משרדי הממשלה (Policy as Code/Infrastructure as Code) – מדיניות מרכזית המחייבת את כלל משרדי הממשלה.

5.2. רכיבים חיוניים לניהול תשתיות מחשוב ארגוני בענן

5.2.1. פלטפורמה לניהול תשתיות מחשוב בענן

- המעבר לענן מאפשר הטמעה של כלים חדשניים ועדכניים לניהול תשתיות מחשוב ויש לו פוטנציאל לצמצם משמעותית את עלויות התפעול והתחזוקה, לקצר את זמני הפיתוח של תוכנה וזמני ההקמה של תשתיות מחשוב ולשפר את השירות למשתמשים השונים בסדרי גודל.
- בענן מתבצעות מגוון פעולות תחזוקת תשתיות באמצעות אוטומציה ואלו מחליפות פעילויות תפעול ותחזוקה המתבצעות לרוב ע"י צוותי תפעול במדרג הנמוך (Low-end). מאידך, פיתוח מהלכי האוטומציה דורש שילוב מיומנויות של אנשי System בכירים עם יכולות פיתוח וחשיבה מערכתית.
- כאשר משלבים בפלטפורמה לניהול תשתיות המחשוב בענן גם פלטפורמות ניהול שירות למשמשי מחשוב (IT Service Management Platform – ITSM), ניתן להגביר את השליטה והבקרה על התשתיות והשירותים בהם נעשה שימוש, ולנהל פעולות רבות בשירות עצמי ואף אוטומטי, תוך שיפור יכולות התמיכה, ניהול ושימור הידע. הדבר מקטין את עלות התפעול וההוצאה הכוללת של הארגון על תשתיות מערכות המידע. חלק מתהליכי

האוטומציה ממומשים ע"ג פלטפורמה זו, ואחרים (המפותחים בטכנולוגיות משיקות) מופעלים הפלטפורמה הכוללת לניהול ענן בממשלת ישראל מתוכה.



הפלטפורמה הכוללת לניהול ענן בממשלת ישראל

- האיור שלהלן מדגים את הארכיטקטורה הפונקציונלית של הפלטפורמה הכוללת לניהול ענן בממשלת ישראל. פלטפורמה זו מכילה איזור נחיתה ורכיבי ניהול ענן חיוניים סביבו, כדוגמת מערכת לניהול זהויות ובקרת גישה (IAM), כלי ניטור והתראות ופלטפורמה ITSM לניהול השירותים. התשתיות והמשאבים המשותפים יאפשרו למשרדי הממשלה עלייה מהירה לענן ללא צורך לממש ולנהל תשתיות אלו עצמאית בכל משרד על כל המשתמע מכך (רכיבים אלו מפורטים בפרק מבוא לפן הטכנולוגי).
- חלק מן הרכיבים בפלטפורמה הם רכיבים הניתנים על ידי ספקיות הענן עצמן (AWS ,Google Cloud) ורכיבים אחרים הם פתרונות צד ג' המשתלבים ופועלים על גבי תשתיותיהם של ספקיות הענן (גם כאשר מדובר בפתרונות "תוכנה כשירות"- SaaS – הם עצמם פועלים על גבי התשתית של ספקיות הענן).
- תפיסת "פלטפורמת ניהול הענן" היא תפיסה כלל ממשלתית והינה חלק מתפיסת המדיניות הממשלתית להתנהלות בענן ציבורי, ללא תלות לשאלה אם היא מיושמת באזור נחיתה ממשלתי או אזור נחיתה משרדי עצמאי. בהתאם לתפיסה זו, איזורי הנחיתה המוקמים על גבי כל ספק הענן מחוברים למספר רכיבים המשותפים ותומכים באופן רוחבי בשירותים הפועלים בענן וממשים מדיניות משותפת.
- "חשבון ענן" ו-איזור נחיתה כתשתית לניהול מערכות מידע ארגוניות בענן
  - לעיתים קיים בלבול בין השימוש במושג "חשבון ענן" ובין המושג איזור נחיתה, ולכן חשוב לחדד את ההבדל בין שני המונחים. כבלל, לכל המשרדים יהיו חשבונות ענן עצמאיים. חשבונות הענן יכולים לפעול כחלק מאזור נחיתה ממשלתי (אליו מחוברים מספר חשבונות ענן של משרדים ממשלתיים) או כחלק מאזור נחיתה משרדי עצמאי. לכל משרד יהיו מספר חשבונות ענן שישמשו לכל הפחות להפרדה בין סביבות השונות, פיתוח, טסט וייצור. משרד יכול להחליט להרחיב את השימוש ולהגדיר חשבונות ענן נוספים בנסיבות מסויימות של גודל ומבנה ארגוני.
  - לעומת המושג "חשבון ענן" – המושג "אזור נחיתה" כפי שתואר לעיל, משמש כדי לתאר סביבת עבודה מתוחמת, מוגדרת מראש וממומשת בקוד, הפועלת ע"ג תשתיות של ספקיות הענן הציבוריים (AWS ו- Goole Cloud). מושג זה מיועד לתאר פתרון שנבנה כדי לקלוט את המערכות המועברות אל הענן על בסיס מדיניות אחידה ומוגדרת מראש, ולאפשר ניהול מחזור החיים מלא ומתועד של תשתיותיהן.

- עם זאת, קיים קשר בין המושג "חשבון ענן ראשי" (Root Account ב- AWS) ובין המושג "אזור נחיתה" בענן, כאשר "חשבון ענן ראשי" הוא מושג ממשי המתאר את יחידת השירות המסופקת ע"י ספק שירותי ענן, כאשר כל יתר המשאבים מוגדרים במסגרתו, בעוד "אזור הנחיתה" הוא מושג קונספטואלי אשר כולל בתוכו אלמנטים שונים של ארכיטקטורת מערכות מידע ארגוניות הפועלות בענן

- בעולם המושגים הספציפי ל-AWS קיים גם המושג Organization והוא מאגד מספר "חשבונות ענן" ומשאבים – Accounts ו- Resources, ובעולם המושגים של Google Cloud החלוקה הפנימית הינה ל- Folders ו- Projects. בעולם של Google Cloud ניתן לקשר להיררכיה אחת מספר Accounts שלכל אחד מהם קיימת כתובת Billing עצמאית, בעוד בעולם של AWS לא קיים פתרון דומה (בעת כתיבת מסמך זה) – כל ה- Accounts המשתייכים לאותו Organization ויש להם Root Account משותף – מחוייבים ע"י כתובת אחת.

- לרוב, יממש "אזור נחיתה" טופולגיה של Hub-and-spoke (כלומר "מרכז" ו-"ענפים") המאגדת מספר חשבונות ענן (Accounts ב- AWS או Folders ו- Projects במושגי Google Cloud) העובדים יחד. לכל חשבון ענן יש הגדרה של ייעוד, שירותים המסופקים על-ידו, ובדומה במסגרת ארכיטקטורת "איזור הנחיתה".

- תפקידו של "אזור הנחיתה" בראש ובראשונה נועד כדי לייצר מדיניות אחידה מלמעלה ולאכוף אותה על כלל "חשבונות הענן". במסגרת זו מוגדרת "מדיניות בסיס" והיררכיה היורשת ממנה, כאשר כל חשבון יכול להוסיף הגדרות.

- איזור הנחיתה מגדיר ארכיטקטורה ושירותים המשותפים למספר "חשבונות ענן" המיועדים לתתי-ארגונים (משרדים), לפרויקטים ו/או מערכות, מגדיר מדיניות והגדרות אבט"מ משותפות ועוד (לרבות האופן בו יתבצע החיבור החיצוני לאינטרנט וממנו ואמצעי אבטחת המידע בהתאם).

- כל רכיבי השירותים הפועלים תחת "חשבונות הענן" במסגרת "איזור הנחיתה" מתוארים כמשאבי ענן (Resources), ולכל משאב כזה ישנן הרשאות המנוהלות עבורו (Authorizations), הגדרות קונפיגורציית "מדיניות ענן" (Policies) אשר חלות עליו, והגדרות של תיוג (Tagging) אשר משמשות את כל מערכות הניטור (Logging), הבקרה (Monitoring), הדיווח והחיוב הכספי (Billing and Charging) בגין השימוש בו.

- "איזורי נחיתה" יכולים להעמיד מגוון של תשתיות תפעול ענן ושירותים משותפים. הם יכולים גם להבטיח עמידה במדיניות ענן (Policies) ובתקני אבטחת מידע משותפים, ולהגביר משילות.

- "חשבון הענן" המשרדי במסגרת "אזור הנחיתה" כולל בתוכו קישורי רשתות וירטואליות המייצרות ענן וירטואלי פרטי במסגרת הענן הציבורי, שרתים, שירותים, אחסון בענן וציודי רשת הפועלים כשירות ע"ג אותן רשתות וירטואליות פרטיות בענן הציבורי, והכי חשוב: הגדרות מדיניות אבט"מ המיושמות עליהם (ובשרתים השונים).

- בהתאם למדיניות הממשלתית הקמה ותחזוקה של "איזורי נחיתה" בממשלת ישראל תתבצע באמצעות קוד בלבד (IaC).

5.2.2. תפיסת ניהול הענן בפרויקט נימבוס

- בהתאם למדיניות מערך הדיגיטל הלאומי, בממשלת ישראל לא יתבצע שימוש ב-"חשבון ענן" שלא באמצעות יישום תפיסת אזור נחיתה, בין אם ממשלתי או משרדי עצמאי, ואין להקים מערכות בענן ציבורי שלא במסגרת אזור נחיתה.

- במטרה לאפשר חסכון ואיגום משאבים – יסופק "איזור נחיתה ממשלתי" לשימושם של משרדי הממשלה על גבי כל אחד מספקי הענן (יפורט בהמשך).

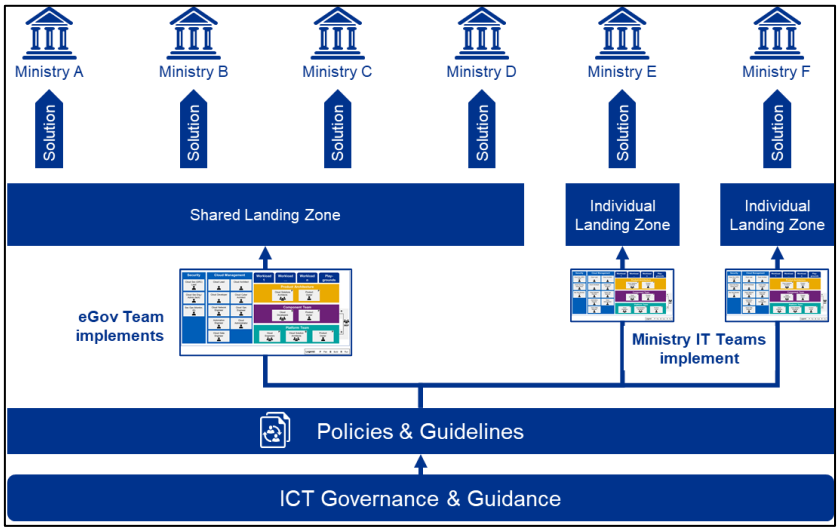
- משרדים הפועלים באמצעות חשבון משרדי יוכלו להקים, לתפעל ולתחזק תשתיות ניהול ענן, הכוללות "איזורי נחיתה" ב- AWS ו/או ב-Google Cloud , בתנאי שעומדים בדרישות הוראת התכ"מ 16.2.2 (יפורט בהמשך) ובכפוף להנחיית יה"ב להקמת אזור נחיתה בממשלה.

- המשרדים שיבחרו לפעול בחשבון עצמאי יידרשו לממש את כל כללי המדיניות הממשלתית במלואם לעבודה בענן, ולפעול בהתאם להנחיות שיתפרסמו מעת לעת בנוגע לטד"מ, רכש, תקצוב, אבטחת מידע והדרכה.

- תחת המדיניות המוגדרת, משרדים יוכלו לעבוד באופן חופשי תוך שליטה מלאה בחשבונות, בשירותים, ברשת, ב- WORKLOADS ושירותי הרשת שלהם, ביישומים ובניהול הפיננסי – בין אם עובדים באזור הנחיתה הממשלתי או באזור נחיתה משרדי עצמאי.
- מערך הדיגיטל הממשלתי יקים מאגר מרכזי שיאפשר שיתוף תבניות (TEMPLATES), קבצי מדיניות (POLICIES AS CODE), IMAGES/CONTAINERS וידע רלוונטי לעבודה בענן.

5.2.3. עקרונות מימוש תפיסת ממשל הענן ברמת המשרד הממשלתי

- משרדי הממשלה והיחידות המונחות על ידי מערך הדיגיטל הלאומי יפעלו באזור נחיתה הפועל בהתאם למדיניות הממשלתית בין אם בשימוש בפלטפורמת ניהול הענן הממשלתית או בין אם בשימוש באזור נחיתה משרדי עצמאי.
- האיור להלן מדגים את מנגנון משילות מדיניות ה- POLICIES המונחלת ע"י מערך הדיגיטל הממשלתי בקרב משרדים המשתמשים באזור הנחיתה הממשלתי ובקרב משרדים המקימים אזור נחיתה משרדי עצמאי:



הסבר לאיור

- בבסיס תפיסת ההפעלה נמצאים ההנחיות ומדיניות החלים על כל משרדי הממשלה ויחידות סמך. מדיניות זו יכולה להיות כתובה במסמך (POLICY AS A DOCUMENT) או מוגדרת טכנית כמדיניות בקוד (POLICY AS CODE).
- בתפיסת ההפעלה מכתיב מערך הדיגיטל מדיניות המחייבת את כלל משרדי הממשלה הנאכפת באיזורי הנחיתה (בין אם מופעלים ע"י מערך הדיגיטל הלאומי ובין אם מופעלים עצמאית ע"י המשרדים), ומדיניות זו מתורגמת טכנית לקבצי מדיניות הפעלה המותקנים ונאכפים טכנית באיזורי הנחיתה באופן היררכי על החשבונות הפועלים במסגרתם.
- בנקודה זו יש פיצול בין משרדים הפועלים באזור נחיתה משרדי עצמאי ובין משרדים הפועלים באזור הנחיתה הממשלתי.
  - באזור הנחיתה הממשלתי תרגום המדיניות הממשלתית לקוד, שמירה על עדכניות והפצת עדכונים למשרדים הינם באחריות מערך הדיגיטל הלאומי. התקנת הקבצים המעודכנים הינה באחריות המשרדים.
  - באזור נחיתה המשרדי תרגום המדיניות הממשלתית לקוד, התקנתו ותחזוקתו (כתוצאה מעדכוני מדיניות) נמצאים באחריות המשרד.
- שירותי תשתית ותמיכה

- משרדים הפועלים באזור הנחיתה הממשלתי מקבלים שירותי תפעול אזור הנחיתה הממשלתי מיחידת הענן ממשלתי של מערך הדיגיטל הלאומי. פירוט השירותים שיינתו על ידי מערך הדיגיטל הלאומי מפורט בפרק מודל חלוקת האחריות.
- משרדים המפעילים אזור נחיתה משרדי עצמאי יקימו צוות תשתיות שיקים ויתחזק את אזור הנחיתה בהתאם להנחיות רלבנטיות ולפירוט בפרק מודל חלוקת האחריות.

5.2.4. עקרונות עבודה ב- Multi-cloud

- בעת בניית פתרונות, על כל משרד להבטיח כי יישמר החופש שלו לבחור ולנייד את היישומים בין ספקי ענן השונים. עובדה זו תבטיח שמירה על עלויות תחרותיות לאורך זמן. יחד עם זאת, יש לבחון סוגיה זו בראייה של סך כל עלות הבעלות (TOTAL COST OF OWNERSHIP). אם שמירה על החופש לבחור ולנייד אפליקציה משמעותה ייקור עלות הבעלות של התחזוקה, התפעול ושירותי הענן, מעבר להבדלים של מחיר השירות בין ספקי הענן – יש להעדיף לממש פתרון שהעלות שלו תהיה גבוהה יותר בעת הצורך לנייד אותו בין ספק ענן אחד למשנהו, אך העלות השוטפת שלו זולה יותר.
- כפי שמוגדר במפורש באסטרטגיית הענן של ממשלת ישראל יש להעדיף תמיד פתרונות SAAS, ככל שהם מספקים מענה לדרישות העסקיות של המשרד. במקרה של שירותי SAAS – הבחירה בספק הענן היא פועל יוצא של הבחירה בפתרון SAAS המסויים, והתלות בספק פתרון ה-SAAS הינה בלתי נמנעת. לפי מכרז נימבוס חייבים פתרונות מבוססי SAAS לפעול על-גבי אחד מספקי הענן שנבחרו ברובד 1 של נימבוס, למעט מקרים בהם הוחרג מדרישה זו הפתרון המסויים ובהתאם למדיניות שתפורסם בנושא.
- במקרה של שירותי PAAS – המפתח לאי תלות בספק ענן מסוים והחופש האמיתי לבחור על איזה פלטפורמה יופעלו כל אפליקציה, WORKLOAD או נתונים – הוא שימוש בכלי פיתוח וטכנולוגיות שאינם ספציפיים לספק ענן מסויים, תוך הבטחת רמת האבטחה ההכרחית הנדרשת (SECURITY FIRST).
- במסגרת מכרז רובד 5 של נימבוס תתאפשר צריכה של שירותים כאלו מתוך קטלוג השירותים הממשלתי של ספקיות הענן.
- גם בחירה בכלי צד ג', המאפשר גמישות בבחירת ספקית הענן, מייצרת תלות, הפעם בספק הפתרונות עצמו. תלות זו איננה שונה במהותה מתלות בספקית שירותי הענן. האופציה היחידה לאי-תלות בבחירת כלי צד ג' היא שימוש בפתרונות קוד פתוח (OPEN SOURCE), אולם הדבר תלוי בפתרונות תמיכה ורישוי חבילות הפצה ושירות ע"י ספקי שירות מתאימים (DISTRIBUTION PACKS).
- במקרה של שירותי IAAS – ההחלטה על איזה ספק ענן להפעיל איזה שירות צריכה לנבוע קודם כל ממניעים כלכליים, תוך מקסום ומיטוב המודל הפיננסי של צריכת שירותי הענן. יחד עם זאת, יש לשים לב למורכבויות תפעוליות וטכנולוגיות רבות הנובעות מעבודה עם יותר מספק ענן אחד, לסיכונים ובעיות הביצועים העשויות להיות כרוכות בכך.
- מידע נוסף על שיקולים בהגירת מערכות לענן ניתן לקרוא בנספח מיגרציה לענן.

6. איזור נחיתה משרדי עצמאי

6.1. עקרונות

- משרדים הפועלים באמצעות חשבון משרדי יוכלו להקים, לתפעל ולתחזק תשתיות ניהול ענן, הכוללות "איזורי נחיתה" ב- AWS ו/או ב-GOOGLE CLOUD, בתנאי שעומדים בדרישות הוראת התכ"מ 16.2.2 .
- כל משרדי הממשלה נדרשים להקפיד על תאימות לתקנים, ההנחיות והמדיניות כפי שהוגדרה על-ידי מערך הדיגיטל הלאומי.
- משרדים אשר יבחרו בתהליך של הקמה עצמאית של אזורי נחיתה יעמידו את כל מעטפת התפעול וההגנה בהתאם להנחיות הגוף המנחה (מערך הסייבר הלאומי או יה"ב).
- הקמה ותחזוקה של "איזורי נחיתה" בממשלת ישראל תתבצע באמצעות קוד בלבד (IaC).
- תפיסת בקרה מרכזית – משרד עצמאי ייצור משתמש בקרה עבור מערך הדיגיטל.
- ניטור מרכזי – חובת העברת לוגים ל-GSOC.
- המשרדים יחוייבו לצרוך פתרונות ממשלתיים מרכזיים .

6.2. מימוש

- מימוש ותחזוקה של אזור הנחיתה המשרדי העצמאי יכול להתבצע ע"י צוות תפעול ענן פנימי של המשרד או תוך הפעלת אחד הספקים הזוכים במכרז התפוקות של דיגיטל-טק (רובד 3 של נימבוס).
- המשרדים הפועלים באזור נחיתה משרדי עצמאי יידרשו לממש את כל כללי המדיניות הממשלתית לעבודה בענן במלואם, ולפעול בהתאם להנחיות שיתפרסמו מעת לעת בנוגע לטד"מ, רכש, תקצוב, אבטחת מידע והדרכה. הכרחי להקפיד על עמידה מלאה בתנאים, אלא אם ועדה ענן במערך הדיגיטל הלאומי אישרה חריג/פטור מפורש וספציפי. המשרדים נדרשים להוכיח יכולות הטמעה והפעלה עקביות, רציפות ויעילות של בקרות האבטחה שתואמות להנחיות מערך הדיגיטל הלאומי.

6.3. שימוש בשירותים משותפים במסגרת איזור נחיתה משרדי עצמאי

- על משרדים המפעילים איזור נחיתה משרדי עצמאי בענן לממש קישוריות מאובטחת מן הרשת המשרדית/חוות שרתים משרדית לספק/י הענן ולאינטרנט. על מימוש זה לעמוד בהנחיית יה"ב ומערך הסייבר הלאומי.

6.4. תצורת עבודה "היברידית" בענן משרדי עצמאי

- על המשרד ליישם פתרון לחיבור לספק הענן מן הרשת המשרדית. קישוריות בין מערכות הפועלות On-prem ובין מערכות הפועלות בענן.
- כל ספקי הענן מציעים כשירות חיבור dedicated בין חוות השרתים המשרדית המקומית (On-prem) ובין חשבון שירותי הענן ו/או באמצעות VPN בפרוטוקול IPSec ע"ג הקישוריות לרשת האינטרנט הציבורית.
- יש לפעול על פי הנחיית יה"ב לנושא הקמת אזור נחיתה.
- חיבור ה-dedicated הנ"ל דומה לחיבור בין הרשת המשרדית ו/או חוות השרתים המשרדית ל-Data Center המופעל ע"י ספק שירותים מנוהלים, Hosting Service Provider או ISP (Internet Service Provider) המספק שירותי אחסון אתרים. גם כאשר החיבור נעשה ע"ג קו תקשורת של ספק כמו "בזק", Hot, Partner או סלקום – הקישוריות בין אתרי הלקוח ממומשת ע"י הקמת רשת וירטואלית העושה שימוש בטכנולוגיה דומה (IPSec).
- העננים הפרטיים הוירטואליים במסגרת הענן הציבורי הינם סגורים לקישוריות לאינטרנט כל עוד הוגדר כך. בהנחה שה- VPC חובר לרשת המשרדית כפי שתואר לעיל, ה- VPC בענן מהווה המשכיות לחוות השרתים

המשרדית. זאת בכפוף לניתוח הסיכונים שיש לבצע בחיבור חוות השרתים המשרדית לענן ובהתאם להנחיות יה"ב בנושא.

- קיימת תפיסה רווחת ומוטעית, לפיה מערכות הפועלות בענן הציבורי מחוברות בהכרח לאינטרנט הציבורי ונגישות לו. סביבת ספק הענן חשופה לאינטרנט הציבורי באופן שונה מהדאטה-סנטר המשרדי בהיבט של סיכוני הסייבר שהיא מייצרת. חשוב להדגיש כי כל עוד לא חובר החשבון בענן הציבורי לאינטרנט – הרשת הינה פרטית, וזאת ככל שהרשת בחוות השרתים המשרדית אליה מחוברות המערכות בחשבון הענן הציבורי איננה מחוברת לאינטרנט מצידה.
- ההגנה הנדרשת על חשבון הענן הציבורי המחובר לרשת בחוות השרתים המשרדית (On-prem) הינה בהתאם לרמת הסיווג של הרשת והמידע המנוהל בה. יש אמצעים שונים שנדרש ליישם ברשת המשרדית העננית, ויש גם מרכיבים דומים. אין הבדל מבחינה זו בין רשת בענן ורשת בחוות-השרתים המקומית (ובלבד שהאיזור בו ממוקמת חוות-השרתים של ספק שירותי הענן הינו בישראל).

6.5. קישור לאינטרנט באזור נחיתה משרדי עצמאי

- גישה לאינטרנט מתוך מערכות המשרדים (E-gress)

משרדים המבקשים לחבר את מערכותיהם הפועלות בענן לצריכת שירותים חיצוניים ו/או לגישה לאינטרנט (גישה זו נקראת E-gress), יעשו זאת באופן ישיר מתוך הרשת הוירטואלית הפרטית שלהם בענן ותוך הקמת פתרון אבטחת המידע המתאים להם. על פתרון זה להתאים לכל היבטי סיווג המידע, ניהול הסיכונים והאיומים שזוהו, פרטיות המידע הנדרשת, ולעלות בקנה אחד עם ההנחיות הישימות במקרה זה (הנחיות יה"ב או מערך הסייבר) וכל ה- Best Practice המקובלים בתחום.

- גישה לציבור (G2B ,G2C) למערכות המשרד באמצעות האינטרנט (In-gress)
  - בתצורה הקיימת (חוות שרתים מקומית), משרדים יכולים לבחור לאחסן את האתרים שלהם והמערכות הנגישות לגישה מהאינטרנט הציבורי ברשת המנוהלת ע"י המשרד עצמו (בחוות השרתים המשרדית), להשתמש בשירותי אחסון אתרים (Hosting Services) המסופק ע"י מערך הדיגיטל הלאומי באופן מאובטח, או להשתמש בשירותי ספק שירותי אחסון אתרים מסחרי חיצוני לממשלת ישראל.
  - בתצורה העתידית, שירות אחסון אתרים שסופק עד כה ע"י מערך הדיגיטל הלאומי יוחלף בניהול עצמאי של שרתים ושירותים ע"ג רשתות ענן וירטואלי פרטי של המשרדים אשר יקושרו לאינטרנט ויאובטחו באחריות המשרדים בהתאם להנחיות המתאימות ומדיניות הסייבר.
  - משרדים המבקשים לחשוף מערכות מסויימות שלהם, הפועלות בענן, לגישה לאינטרנט (גישה זו נקראת In-gress) – יעשו זאת בהתאם למדיניות יה"ב. זאת, בהתאם לניהול הסיכונים, לאיומים הקיימים, לפרטיות המידע הנדרשת, להנחיות הישימות לגביהם (הנחיות יה"ב או מערך הסייבר) וכל ה- Best Practice המקובלים בתחום.

7. איזור הנחיתה הממשלתי

7.1. רקע להקמת אזור נחיתה ממשלתי

- הפעלת "חשבון ענן" היא תהליך הדורש ידע מקצועי, משאבים והבנה בתחום, ובהתאם לכך נושא בחובו סיכונים רבים, לרבות בתחומי הסייבר ואבטחת המידע. במסגרת אסטרטגיית הענן של ממשלת ישראל מוגדרים עקרונות של שיפור האפקטיביות וייעול ההוצאה הממשלתית בתחום הטכנולוגיה, וכן הבטחת המשילות, הריבונות וההגנה בסייבר על התשתיות הטכנולוגיות והמידע הממשלתי בענן.

- איזור הנחיתה הממשלתי מגלם תפיסה של שיתופיות (COLLABORATION), איגום משאבים וגיבוש של צוותי ענן מרכזיים, ויפחית את נטל המשאבים ממשרדי הממשלה.
- משרדים שישתמשו בפלטפורמה זו ייהנו מכל מעטפת ההגנה והתפעול ללא צורך להקימה בעצמם או להעמיד צוותים על מנת לתחזק אותה.
- התפיסה מאפשרת למשרד מיקוד בפעילותו העסקית בסביבה המשרדית כאשר התפעול של איזור הנחיתה מבוצע עי מערך הדיגיטל.
- תפיסת המימוש של איזור הנחיתה הממשלתי, מפרידה בין תשתיות משותפות ומשאבים משותפים, הנמצאים בניהול מרכזי, ובין חשבונות ענן ומשאבי ענן של משרדי הממשלה – הנמצאים בניהולם התפעולי העצמאי.
- אזור הנחיתה הממשלתי יתופעל על-ידי מערך הדיגיטל הלאומי ויכיל חשבונות שונים לשימושם של משרדי ממשלה רבים (על גבי שני ספקי הענן שנבחרו ברובד 1 של נימבוס: AWS ו- GOOGLE CLOUD). איזור הנחיתה הממשלתי מהווה חלק מ- "פלטפורמת ניהול הענן הממשלתית" המסופקת ע"י מערך הדיגיטל הלאומי למשרדי הממשלה כשירות מנוהל.
- השירות המנוהל של פלטפורמת ניהול הענן הממשלתית כולל הטמעה של פתרון אזורי הנחיתה הרב-ענני המרכזי בסביבה מתקדמת שמבטיחה ניהול הולם של כל הבלים והתהליכים הקשורים לענן, לרבות הרכיבים הבאים: קישוריות מאובטחת לאינטרנט, ניהול שירותי IT (ITSM), ניהול שירותי ענן, ניהול זהויות וגישה (IAM), כלי ניטור והתראה, מרכיבי אבטחה ומרכיבי רשת.

7.2. עקרונות ומימוש

- פלטפורמת ניהול הענן הממשלתית הנה נקודת התחלה שממנה המשרד יכול להקים במהירות סביבות מאובטחות לטובת שירותים ופרויקטים, להפעיל ולפרוס במהירות יישומים, כל זאת בסביבה מאובטחת ומנוהלת, מרובת מערכות, פרויקטים ותתי-יחידות ארגוניות עצמאיות. הקמת הסביבות ואיזורי הנחיתה מתבצעת כשירות המסופק ע"י מערך הדיגיטל הלאומי.
- יתרונות מרכזיים של שימוש בפלטפורמת ניהול הענן הממשלתית (כמו בכל שימוש בתשתית משותפת בממשלה) הוא התחזוקה השוטפת המרכזית של איזור הנחיתה, ויכולתה לתת מענה מרכזי עדכני ומהיר לדרישות הממשלה, הרגולציה וניהול סיכונים, החיבור האינטגרלי לשירותים ממשלתיים משותפים (כמו קישוריות מאובטחת לענן, קישוריות מאובטחת לאינטרנט וממנו למערכות של המשרד) והחיבור המובנה לשירותים רוחביים שונים (דוגמת ניהול זהויות – IAM/IDP, דוא"ל ממשלתי, שדרת המידע הממשלתית וכדומה).
- בתוך פלטפורמת ניהול הענן הממשלתית יוכלו משרדים לצרוך ולהגדיר פתרונות העושים שימוש בשירותי ענן זמינים שהוגדרו ואושרו על ידי ה- CCOE בקטלוג שירותי הענן, תוך כדי שמירה על מדיניות והנחיות המיושמות באזור הנחיתה המנוהל על ידי מערך הדיגיטל הלאומי. זאת, כדי להבטיח משילות, עמידה בנהלים, כללי מדיניות אבטחת מידע, תאימות ואחידות בין כל משרדי הממשלה, כמו בשימוש בכלי פיתוח, בדיקה, ניטור, תחזוקה, תפעול, ניהול הייצור ועוד.
- במסגרת פלטפורמת ניהול הענן הממשלתית יוקמו "איזורי נחיתה" הפועלים הן על גבי AMAZON WEB SERVICES ועל GOOGLE CLOUD SERVICES במקביל. "איזורי הנחיתה" יכללו את חשבונות הענן הציבורי המשרתים את משרדי הממשלה. בתוך איזורי הנחיתה תוקם היררכיה של חשבונות. כאשר החשבון העליון הינו של יחידת הענן במערך הדיגיטל הלאומי ולכל משרד יוקמו חשבונות ענן (בהתאם ל BEST PRACTICE של סביבות עבודה) לשימוש המשרד בהתאם לצורך העסקי שלו.
- בתוך כל חשבון ענן ציבורי משרדי השייך לפטפורמת הענן הממשלתית יוקמו עננים פרטיים וירטואליים אשר יקושרו לחשבונות ענן אחרים על פי הצורך.
- על-גבי העננים הפרטיים הוירטואליים בענן הציבורי יוקמו שירותים ומשאבים שונים (IAAS, PAAS וכו').

- בהתאם לעיקרון העצמאות התפעולים של המשרדים – הקמת השירותים והמשאבים בעננים הפרטיים הוירטואליים של המשרדים בחשבונותיהם תתבצע ע"י המשרדים עצמם.
- משרדים המשתלבים במסגרת "איזור הנחיתה הממשלתי" המהווה חלק מפלטפורמת ניהול הענן הממשלתית יוכלו להשתמש בחשבונות שלהם תוך שליטה מלאה בחשבונות, בשירותים, ברשת, ב- WORKLOADS שלהם, ביישומים ובניהול הפיננסי שלהם.
- באזור נחיתה הממשלתי יוגדרו חשבונות ענן בהתאם להנחיות וסטנדרטים שייקבעו על ידי ה CCOE. יחד עם זאת קיימת הבנה שישנם מקרים שלמשרד קיים צורך עסקי שחורג מההמדיניות הכלל ממשלתית. דרישות אלו יש להפנות ליחידת ה -CCOE.
- לאחר הטמעת כלי ITSM במסגרת פלטפורמת ניהול הענן הממשלתי, כל הגישה לניהול התפעול והשירות תתבצע באמצעות פורטל לשירות עצמי.
- בעתיד, תפותח תשתית אוטומציה להקמת שירותים ומשאבי ענן תוך "תזמור" (ORCHESTRATION) של שירותי רשת שונים, אשר הגישה אליה תתבצע ע"י הגשת בקשת שירות בפורטל השירות של פלטפורמת הניהול.
- תהליך העמדת השירות המבוקש (FULFILLMENT) יהיה אוטומטי, ידני או חצי-אוטומטי, תלוי בשירות המבוקש ובנקודת הזמן בהתפתחות פלטפורמת ניהול הענן הממשלתית.
- צוות הקמת ותחזוקת פלטפורמת ניהול הענן הממשלתית של מערך הדיגיטל הלאומי יהיה אחראי לשיפור מתמיד של פורטל השירות, תהליכי האוטומציה ותזמור אספקת השירות במסגרתו, לטובת הנגשת יכולות הענן לכלל משרדי ממשלת ישראל ושיפור מתמשך של העמידה במדדי SLA המסופקים.

7.3. שימוש בשירותים משותפים במסגרת איזור נחיתה הממשלתי

- שירותים משותפים מנוהלים ברמה הממשלתית מאפשרים להשתמש בשיטות עבודה מומלצות (BEST PRACTICES) בתחומי הליבה, כגון אבטחה, וקישוריות לאינטרנט ויכולת עבודה היברידית (קישוריות מה- ON PREM לענן), וכן מספקים למשרדי הממשלה קטלוג שירותי ענן זמינים.
- במסגרת השימוש בשירותים המשותפים מסופקת תשתית חיבור מאובטחת בין הרשת הממשלתית (ON-PREM) לעננים שזכו במכרז נימבוס (AWS, GOOGLE CLOUD), לכל ספק ענן יסופק קישור יעודי.

7.4. תצורת עבודה "היברידית" באזור הנחיתה הממשלתי

- המושג "היברידית" מתאר את קישוריות בין מערכות הפועלות ON-PREM ובין מערכות הפועלות בענן.
- משרדים שיעבדו על גבי פלטפורמת ניהול הענן הממשלתי יקבלו פתרון סטנדרטי לחיבוריות של ערוץ התקשורת שלהם המקשר בין הרשת הפרטית הפיזית ב- DATA CENTER שלהם במתקן המחשב ON-PREM ובין הרשת הענן הפרטי הוירטואלי באיזור הנחיתה.
- החיבור הנ"ל פרטי לחלוטין ואף כי איזור הנחיתה מנוהל ע"י מערך הדיגיטל הלאומי הנתונים המועברים בין חצרי לקוח והרשת הפרטית של המשרד מועברים על גבי VPN מאובטח לכל TUNNEL VPN יהיה גיבוי ע"מ להבטיח שרידות גבוהה של החיבוריות בין המשרד לענן.
- ענן פרטי וירטואלי VPC של משרד ממשלתי משמש הרחבה של הרשת המשרדית הפנימית. משרדים העושים שימוש בפלטפורמת ניהול הענן הממשלתית המופעלת ע"י מערך הדיגיטל הלאומי יקבלו כשירות משותף את קישור הרשת הפרטית שלהם בענן לרשת המשרדית שלהם.
- לא כל VPC פרטי של משרד ממשלתי חייב להיות מחובר לרשת המשרדית, ולא כל VPC חייב להיות מחובר לאינטרנט. ניתן לייצר הפרדה בין מספר VPC שיועמדו לרשות משרד ממשלתי, כאשר VPC אחד יקושר לרשת המשרדית ו- VPC אחר יקושר "החוצה" לאינטרנט (E-GRESS).

- לא כל VPC פרטי בענן של משרד ממשלתי חייב להיות מחובר לרשת המשרדית, ולא כל VPC המקושר "החוצה" לאינטרנט (E-GRESS) חייב להיות גם מקושר "פנימה" לצורך גישה מן האינטרנט ליישומי המשרד (IN-GRESS). בהתאם למדיניות הממשלתית יש לייצר הפרדה בין VPC שיקושר לרשת המשרדית ו- VPC שיקושר לאינטרנט לצורך גישה "פנימה" (IN-GRESS). ע"י זה נוצרת ארכיטקטורת חיבור דמויית DMZ כלפי חוץ.

7.5. קישור לאינטרנט באזור הנחיתה הממשלתי

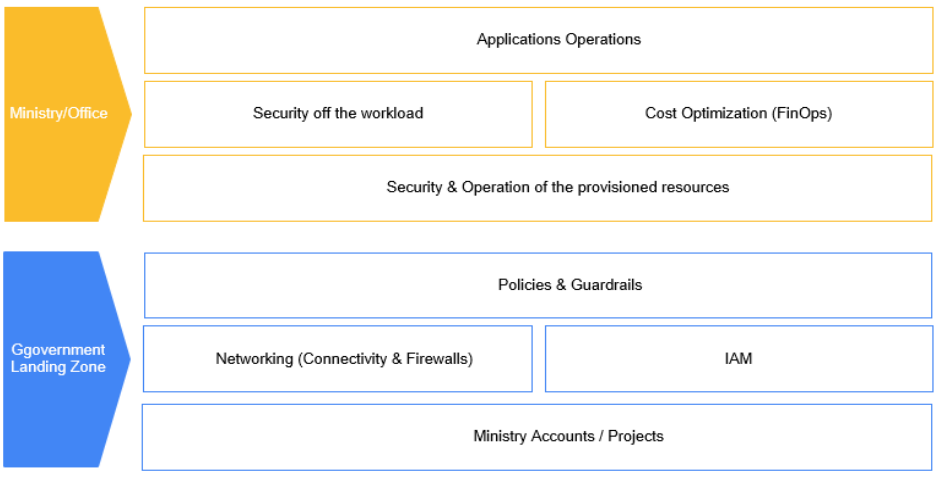
- גישה לאינטרנט מתוך מערכות המשרדים (E-GRESS)
  - בתצורת איזור נחיתה ממשלתי המהווה חלק מפלטפורמת ניהול הענן הממשלתית – הגישה "החוצה" מתוך רשתות המשרדים לשירותים חיוניים הפועלים באינטרנט סגורה כברירת מחדל.
  - מערך הדיגיטל יאפשר קישוריות E-GRESS עבור משרדים הפועלים באזור הנחיתה הממשלתי. משרדים שישתמשו באזור הנחיתה הממשלתי יקבלו קישוריות "החוצה" לאינטרנט כשירות מאובטח.

  לצורך זה יש להגיש בקשה לחיבור הרשת של הענן הפרטי הוירטואלי של המשרד, לשירות המשותף של קישוריות מאובטחת לאינטרנט (E-GRESS).
- גישה לציבור (G2B ,G2C) למערכות המשרד באמצעות האינטרנט (IN-GRESS)
  - בתצורה הקיימת (ON PREM), משרדים יכולים לבחור לאחסן את האתרים שלהם והמערכות הנגישות לגישה מהאינטרנט הציבורי ברשת המנוהלת ע"י המשרד עצמו (בחוות השרתים המשרדית), להשתמש בשירותי אחסון אתרים (HOSTING SERVICES) המסופק ע"י מערך הדיגיטל באופן מאובטח, או להשתמש בשירותי ספק שירותי אחסון אתרים מסחרי חיצוני לממשלת ישראל.
  - בתצורה העתידית, שירות אחסון אתרים שסופק עד כה ע"י מערך הדיגיטל הלאומי יוחלף בניהול עצמאי של שרתים ושירותים על גבי רשתות ענן וירטואלי פרטי של המשרדים אשר יקושרו לאינטרנט ויאובטחו באחריות המשרדים בהתאם להנחיות המתאימות ומדיניות הסייבר כפי שתפורסם.
  - באיזור הנחיתה הממשלתי החיבור של רשתות ענן וירטואלי פרטי של המשרדים לאינטרנט איננו זמין כברירת מחדל.

7.6. יש לשים לב לשתי מודלים להגדרת האחריות:

- מודל אחריות משותפת בין ספק הענן ללקוח
- מודל חלוקת האחריות בין מערך הדיגיטל ובין המשרד הממשלתי

התרשים הבא מציג באופן גרפי את שכבות של חלוקת האחריות בן אזור נחיתה ממשלתי לבין שכבות באחריות משרד שנמצא באזור הנחיתה הממשלתי.



8. איזור נחיתה ממשלתי ואיזור נחיתה משרדי עצמאי – תרחיש משולב

קיימים מצבים בהם משרדים יעבדו בפלטפורמת ניהל הענן הממשלתי ובמקביל יקימו פרויקטים שיפעלו תחת אזור נחיתה עצמאי, או להיפך. מספר תרחישים לדוגמה:

- עבודה עם ספק של שירותים מנוהלים (MSP – MANAGED SERVICE PROVIDER) אשר יש לו אחריות כוללת על מערכת או שירות מסוים במסגרת הסכם ההתקשרות פרטני עימו, הפועל במודל עיסקי הכולל את תשלום החשבון לספק שירותי הענן של נימבוס. יש לציין, כי בהתאם למכרז נימבוס, גם ספקי שירותים מנוהלים אשר מספקים שירותים לממשלה בחשבון עצמאי זוכים לתנאי נימבוס בשירותי הענן בהתאם למפורט בהודעת המכרז.
- מיקור חוץ מלא או חלקי של שירותי תפעול תשתיות מערכות המידע של המשרד, והתחייבות של ספק שירותי מיקור החוץ לרמת שירות (SLA) ייחודית המוסכמת איתו חוזית ופרטנית. חשוב לציין, כי לא כל מיקור חוץ מהווה סיבה מספקת לעבודה בחשבון עצמאי, אלא רק כאשר ספק שירותי מיקור חוץ אחראי להפעיל חוות שרתים משרדית עבור המשרד, ותנאים נוספים בהם מחוייב לעמוד המשרד המפורטים בהוראות התכ"מ הרלוונטית.

בשני המקרים החשבון נמצא בבעלותו של ספק חיצוני לממשלה ולא בידי המשרד עצמו, והוא הגורם המחוייב מול המשרד לעמוד בתנאים לניהול חשבון ענן עצמאי.

על הגורם שבבעלותו החשבון מוטלת האחריות להטמיע את מדיניות תפעול הענן המוכתבת ע"י מערך הדיגיטל הלאומי, לעמוד בתנאי הוראת התכ"מ 16.2.2 לניהול חשבון ענן עצמאי, וכמו-כן להתייחס לשקולי התצורה הקיימת באותו משרד ובשיקולי "ריבוי עננים" (MULTI-CLOUD).

9. מודל חלוקת האחריות

פרק זה מגדיר את מודל חלוקת האחריות בממשלה בהתייחס להקמה, תפעול ושימוש באזור נחיתה בהקשר לכל אחת מהחלופות – עבודה על גבי אזור הנחיתה הממשלתי או יישום אזור נחיתה משרדי עצמאי. הטבלה מגדירה את חלוקת האחראיות בין המשרד ובין מערך הדיגיטל הלאומי, מנהל הרכש ומערך הסייבר הלאומי ומתייחס לשני המקרים הבאים:

- משרד הנמצא באזור הנחיתה הממשלתי
- משרד באזור נחיתה בהקמה עצמאית

הנושאים המפורטים בטבלה:

- אוטומציה וניהול משאבים בענן
- אבטחת מידע וקישוריות
- ניהול זהויות
- שירותים משותפים
- ניטור
- פיתוח ותחזוקת יישומים בענן
- FinOps

טבלת מודל חלוקת האחראיות

נושא	משרד באיזור נחיתה ממשלתי	משרד באיזור נחיתה משרדי עצמאי	הערה
אוטומציות וניהול משאבים בענן			
הקמת חשבונות ופרויקטים למשרד	מערך הדיגיטל	המשרד	עד ליישום פתרון ITSM על המשרד להעביר דרישה של כמות פרויקטים/חשבונות, ציון חלוקת הפרויקטים וציון ה owner של הפרויקטים
הקמה ותפעול משאבי תשתיות מחשוב (PaaS, IaaS, Networking, Security) - פריסת שירותים בתוך הפרויקטים / חשבונות - בתוך המשרד	המשרד	המשרד	בעתיד יהיה קטלוג של תהליכי הקמה ותפעול משאבי תשתית מחשוב זמין בפורטל ה- ITSM
אוטומציה של תהליכי הקמה ותפעול משאבי תשתיות מחשוב - הניתנים להפעלה באמצעות פורטל ITSM	מערך הדיגיטל	המשרד	עתידי - יוקם בהמשך
הטמעת תיוגים בסיסיים ב- Policy הממשלתי	מערך הדיגיטל	המשרד	מערך הדיגיטל מנחה ומתריע בנושא מדיניות התיוג
הרחבת תיוגים בכפוף להנחיות	המשרד	המשרד	מערך הדיגיטל מנחה ומתריע בנושא מדיניות התיוג
הקמה, תפעול ותחזוקת DevOps (יישומי המשרד)	המשרד	המשרד	
הקמה, תפעול ותחזוקת תשתיות פנים-משרדיות	המשרד	המשרד	
גיבוי אחסון (Backup)	המשרד	המשרד	
ניהול קטלוג של Images / סביבות פיתוח משרדי	מערך הדיגטל המשרד	מערך הדיגיטל המשרד	עתידי
ניהול קטלוג של Images / סביבות פיתוח ממשלתי	מערך הדיגיטל	-	עתידי נדרשת בחינה של שיתוף הקטלוג גם למשרדים עצמאיים
ניהול טלאי תוכנה (Patch Management)	המשרד מערך הדיגיטל	המשרד	הטלאת שירותים משותפים תתבצע ע"י מערך הדיגיטל. הטלאת שירותים ויישומים של המשרדים תתבצע

			מתוך פתרון ניהול והפצת טלאים מרכזי (עתידי – יעודכן בהמשך). נדרשת בחינה של שיתוף הפתרון גם למשרדים עצמאיים
SBOM פנים ממשלתי	מערך הדיגיטל	מערך הדיגיטל	עתידי
הקמת קטלוג MarketPlace ממשלתי לצריכת שירותים בהתאם להנחיות מנהל הרכש	מערך הדיגיטל	המשרד	עתידי יבוצע באמצעות פתרון ITSM
ניהול אוטומציה של תהליך צריכת שירותים מתוך הקטלוג הממשלתי (Marketplace)	מערך הדיגיטל	המשרד	המשרד פונה בבקשה לצריכת שירות
אבטחת מידע וקישוריות			
פתרון מאובטח ליציאה לאינטרנט (גלישה ופנייה לשירותים חיצוניים מתוך VPC בענן)	מערך הדיגיטל	המשרד	קיים
פתרון מאובטח לחשיפת שרתים ושירותים לאינטרנט כולל הגנות WAF LB, DDOS ועוד (הפתרון באזור הנחיתה הממשלתי מחליף את שירותי אחסון האתרים של ממש"ז ויישומי G2C, G2B)	מערך הדיגיטל	המשרד	עתידי
הגנה פנימית על מערכות, שרתים ואפליקציות ברמת המשרד	המשרד	המשרד	כל משרד צריך לאבטח את מערכותיו במעגל פנים-ממשלתי. (בנוסף להגנה הקיימת במסגרת אזור הנחיתה הממשלתי)
ניהול חוקי Firewall ברמת המשרד	המשרד	המשרד	
קישור מאובטח בין VPC של משרדים בענן לרשת On-prem	מערך הדיגיטל המשרד	המשרד	עתידי
קישור מאובטח בין חשבונות/פרויקטים בסביבה סגורה ל- VPC פתוח לאינטרנט	מערך הדיגיטל	המשרד	עתידי
קישוריות מאובטחת בין סביבות שונות (בין VPC ל- VPC) בחשבונות של אותו המשרד באותו רמת אבטחה. (לדוגמה Dev-Test/Staging-Prod)	המשרד	המשרד	Pipeline - ייבחן הקמה של בשירות משותף – עתידי
הקמה ותחזוקה של פתרונות אבטחת המידע בתוך הענן המשרדי (חשבונות המשרד)	המשרד	המשרד	
הפקת מדיניות אבטחת ענן טכנית (Policy) והפצתה למפעילי אזורי נחיתה	מערך הדיגיטל	מערך הדיגיטל	קיים
פריסת מדיניות אבטחת ענן טכנית (Policy) עד רמת המשרד	מערך הדיגיטל	המשרד	קיים

פריסת מדיניות אבטחת ענן טכנית (Policy) ברמת המשרד ומטה	המשרד	המשרד	בנוסף למדיניות הממשלתית
ניהול בקרות וציות (Compliance Control Management)	המשרד (בפיקוח מערך הדיגיטל)	המשרד (בפיקוח מערך הדיגיטל)	עתידי – ייושם באמצעות תהליכי Policy Lifecycle Management של פתרון ה- ITSM
ניהול זהויות			
הגדרה ותפעול חשבונות משתמשים, קבוצות וזהויות	המשרד	המשרד	עד ליישום פתרון IAM ממשלתי, על המשרד להעביר את הבקשות למימוש באמצעות צוות תפעול הענן של מערך הדיגיטל
יישום וניהול מוצר ניהול זהויות (IAM)	מערך הדיגיטל	המשרד מערך הדיגיטל	עתידי – ייבחן בהמשך אופן יישום
שירותים משותפים			
הקמה תפעול וניהול של IaC Repository	מערך הדיגיטל	המשרד מערך הדיגיטל	עתידי – יוקם בהמשך
הקמה, תפעול ותחזוקת API Management	המשרד מערך הדיגיטל	המשרד מערך הדיגיטל (ברמת המדיניות - policy)	פתרונות בבחינה - יעודכן בהמשך.
קישוריות לשדרת המידע הממשלתית (API, MFT, Event Driven)	מערך הדיגיטל	המשרד מערך הדיגיטל	פתרונות בבחינה - יעודכן בהמשך
כלי לניהול ואוטומציה של טיפול בתקלות ואירועים	המשרד מערך הדיגיטל	המשרד	עתידי – ייושם באמצעות תהליכי Service Management של פתרון ה- ITSM
ניטור			
ניטור ובקרת רשת ותשתית	המשרד מערך הדיגיטל	המשרד מערך הדיגיטל	עתידי – פתרונות בבחינה - יעודכן בהמשך
הקמת ניטור אפליקטיבי למערכות בתוך פרויקטים / חשבונות	המשרד	המשרד	
איגום כלל הלוגים התשתיתיים של כלל החשבונות לתוך מאגר לוגים מרכזי	המשרד (בפיקוח מערך הדיגיטל)	המשרד (בפיקוח מערך הדיגיטל)	נמצא בבחינה המדיניות לניטור כלל ממשלתי בהתאם למדיניות יה"ב
מדידה וניטור ביצועי יישומים	המשרד (בפיקוח מערך הדיגיטל)	המשרד (בפיקוח מערך הדיגיטל)	בהתאם למדיניות יה"ב

שמירה מקומית (בחשבון הלקוח) של audit logs אפליקטיביים המחויבים לשמירה לתקופה ארוכה על פי רגולציה	המשרד (בפיקוח מערך הדיגיטל)	המשרד (בפיקוח מערך הדיגיטל)	
SOC ממשלתי	המשרד (בפיקוח מערך הדיגיטל)	המשרד (בפיקוח מערך הדיגיטל)	חלוקת אחריות תוגדר בהנחיות יה"ב
SOAR (אוטומציה של זיהוי וטיפול באירועים)	המשרד (בפיקוח מערך הדיגיטל)	המשרד (בפיקוח מערך הדיגיטל)	עתידי
פיתוח ותחזוקת יישומים בענן			
פיתוח יישומים ומערכות	המשרד	המשרד	
אחריות למידע ונתונים (לרבות סיווג, זיהוי רגולציה רלוונטית, הגנה, בקרת ציות להנחיות וגיבוי)	המשרד	המשרד	
שליחת לוגים אפליקטיביים לחשבון הלוגים המשרדי המרכזי	המשרד	המשרד	
הקמת גיבוי ושרידות למערכות (DR, Failover & HA)	המשרד	המשרד	
FinOps			מדיניות ה Billing בענן נמצאת בחינה של החשב"ל
חיוב וגביה	מערך הדיגיטל מנהל הרכש המשרד	מנהל הרכש המשרד	כלי מרכזי מנהל את תהליך ההתחשבנות (עתידי - פתרונות בבחינה - יעודכן בהמשך)
תהליך הקמת החשבון ב- Google Cloud לצורכי Billing	המשרד	המשרד	
חיוב וגביה שירותים משותפים	בבחינה	בבחינה	בבחינה

10.שירותים רוחביים

10.1. עקרונות

התשתיות הבאות יוקמו כשירותים ממשלתיים רוחביים, בהתאם להחלטת ממשלה 231:

- תשתית לניהול הדואר האלקטרוני הממשלתי
- תשתית לניהול זהויות
- תשתית לניהול ושיתוף מסמכים

פלטפורמת ניהול הענן הממשלתית תטמיע בתוכה את השירותים הנ"ל ושירותים משותפים נוספים, לדוגמה: חיבור ל-SOC הממשלתי ,פלטפורמה מרכזית כמו SIEM או IAM, ITSM, שדרת המידע הממשלתית בענן, פתרונות SaaS מאושרים שיאושרו לשימוש ע"י ה- CCoE ועוד.

10.2. חיבור לשירותים רוחביים למשרדים באזור נחיתה משרדי עצמאי

משרד שהקים איזור נחיתה משרדי עצמאי ונדרש לעשות שימוש בשירותים רוחביים אלו נדרש לבנות פתרון חיבור כלקוח חיצוני לאיזור הנחיתה הממשלתי כדי להשתמש בשירותים הרוחביים. משרדים שאינם חלק מפטפורמת ניהול הענן הממשלתי יכולים לצרוך שירותים אלה או שירותים אחרים שיוצעו ע"י משרדים ממשלתיים לשימוש משרדים אחרים, זאת באמצעות שדרת המידע הממשלתית בענן או פלטפורמות נוספות שיוקמו בעתיד.

נושא זה נמצא בבחינה ויתפרסמו הנחיות פרטניות בהמשך.

10.3. חיבור לשירותים רוחביים למשרדים באזור נחיתה ממשלתי

ההתחברות לשירותים הרוחביים הנ"ל תתבצע באופן אינטגרטיבי מתוך פלטפורמת ניהול הענן הממשלתית. שדרת המידע הממשלתית בעידן הענן

10.4. שדרת המידע הממשלתית

- "שדרת המידע הממשלתית" כיום הינה פתרון מרכזי של API Management אשר הופעל בממשלה (במערכת On-prem במקור) כדי לספק מענה בין היתר לרגולציה הממשלתית למימוש העברת מידע לצורך קידום מדיניות Ask Once תוך עמידה בתקנות הגנת הפרטיות. הפתרון מייצג תפיסה נפוצה בארגונים לפיה כל משרד המבקש לחשוף שירותי מידע לרשות לקוחות חיצוניים יעשה זאת באופן סטנדרטי וניתן לניהול, ובאותו אופן – כל משרד המעוניין לצרוך שירותי מידע לצורך תהליכים רוחביים פנים-ממשלתיים יעשה זאת תוך גישה לאותה תשתית, כאשר תיעוד ה- API וכל השליטה והניהול שלו מתבצעים דרך ממשק פורטל מרכזי.
- שדרת המידע הממשלתית תורחב לענן במסגרת פרויקט נימבוס, ומשרדים יוכלו לעשות בה שימוש כדי לשתף מידע האחד עם השני בענן וכן בין הענן למערכות הפועלות On-prem ולהיפך.
- בפתרון שדרת המידע הממשלתית בענן יעשה שימוש ברכיב API Gateway אשר יותקן בכל אחת מהרשתות המשרדיות הפרטיות באיזור הנחיתה בענן, אליו יופצו קבצי מדיניות ענן טכנית (Policy files) התואמים את מדיניות הענן הממשלתית וקיבלו אישור יה"ב.
- בארכיטקטורה המותאמת לענן תפיסת הניהול היא תפיסה מבוזרת בה לכל משרד יש יכולת ניהול עצמית ומצופה ממנו לנהל את הרכיב שלו באמצעות פורטל ניהול מרכזי ולפרסם בו באופן עצמאי שירותים שברצונו לחשוף, בין אם ללקוחות ממשלתיים (G2G), או למשתמשים ולקוחות חיצוניים לממשלה (G2C, G2B).

- למעשה, בענן מתבטלת האבחנה בין שירותי G2G ושירותי G2C – על משרד החושף שירותים להגדיר מי הוא קהל היעד של כל שירות ושירות בעת פרסומו והגדרת קובץ מדיניות הענן הטכנית של השירות (POLICY FILE).
- ברמת רשת התקשורת, רכיבי ה- API GATEWAYS של כל משרד ומשרד יעבדו ישירות מול רכיבי ה- API GATEWAYS במשרדים האחרים. פתרון אבטחת המידע לנושא זה יתואר במסגרת מסמך מדיניות הסייבר בנימבוס של ה- CCOE.
- ניטור התעבורה ב- API GATEWAY המשרדי יתבצע ע"י איסוף קבצי AUDIT LOG ברמה המשרדית וברמה הממשלתית כאחד.
- טכנולוגיית ה- API MANAGEMENT אשר עומדת בבסיס שדרת המידע הממשלתית תשתלב גם במסגרת קישוריות הענן ההיברידי בין מערכות הפועלות בחוות השרתים המשרדיות ובין מערכות הפועלות בענן הממשלתי.
- בעתיד ינוהלו במסגרת שדרת המידע בענן פתרונות מתקדמים של קטלוג של שירותים הנגישים באמצעות API, לניהול הרשאות גישה ללקוחות וניטור התפוצה של מידע המסופק ממאגרי המידע הממשלתיים לגורמים השונים.
- פתרון ניהול האינטגרציה באמצעות ה- API MANAGEMENT יהיה הבסיס לתשתית שתאפשר חיבור לספקי פתרונות SAAS, לרבות ספקי שירותי צד ג' מאושרים לשימוש ע"י ה- CCOE.
- הפצת מדיניות טכנית (POLICY BY FILE) לרכיבי ה- API MANAGEMENT:
  - שדרת המידע הממשלתית הינה שירות רוחבי המסופק לכלל משרדי הממשלה. המדיניות הטכנית (Policy Files) תופץ לכלל המשרדים.
  - עבור משרדים שיעשו שימוש באזור הנחיתה הממשלתי תותקן המדיניות ותוטמע ברכיבי ה- API Management המשרדיים באופן אוטומטי.
  - משרד שהקים איזור נחיתה משרדי עצמאי יידרש לבנות פתרון חיבור ייחודי בלקוח חיצוני לאיזור הנחיתה הממשלתי וייצטרך להתאים את קבצי המדיניות, להתקין ולהטמיע שינויים באופן עצמאי.

11. יישום ריבוי עננים (Multi-cloud)

11.1. תמיכה ב- Multi-cloud

- יכולת עבודה בשקיפות בריבוי-עננים, על גבי תשתיות של שני ספקי הענן הזוכים (Multi-cloud), מתאפשרת בעזרת יישום של תפיסת פלטפורמת ניהול הענן. כפי שתואר בפרק העקרונות, תפיסה זו כוללת מימוש של חיבור אזורי הנחיתה בכל אחד מספקי הענן לרכיבים מושתפים של: IAM, פלטפורמת ITSM (כולל CMDB), פתרונות Log & Audit, פתרונות FinOps ו- Security Monitoring.

11.2. איזור נחיתה משרדי עצמאי

- משרדים שיקימו איזור נחיתה באופן עצמאי יצטרכו להבטיח את תמיכת התשתיות שלהם ב- Multi-cloud, וליישם פתרון עצמאי של פלטפורמת ניהול ענן ובו תשתיות ניהול ענן המאפשרות גישה אחידה להזדהות, שליטה, בקרה וניהול ענן באופן אחיד בשני העננים.

11.3. עבודה באזור הנחיתה הממשלתי

- משרדים שיפעלו באמצעות פלטפורמת ניהול הענן הממשלתית יהיו בעלי גישה לחשבונות בכל אחד מספקי הענן.
- על מנת להקל על המשרדים לעבוד באופן פשוט ואחיד באזורי נחיתה השייכים לספקי ענן שונים – מומש איזור הנחיתה הממשלתי כתומך ב-Multi-cloud כחלק מתפיסת העיצוב הבסיסית של הפתרון. משרדים שיעשו שימוש בפתרון זה יעבדו בגישה אחידה לניהול הענן ובכלי ניהול, שליטה ובקרה אחידים בשני העננים.

11.4. פירוק של מערכת מידע לתתי-מערכות/רכיבי-מערכת הפועלים בעננים שונים

- "פתרון בית-הספר" של פריסת מערכות מידע בענן גורס שעל כל רכיבי המערכת לפעול באותו ענן, על מנת להפחית שיהוי ובעיות אינטגרציה, זמינות ותקשורת.
- במקרים מסויימים נפרק מערכת מידע אחת לרכיבים שיפעלו בעננים שונים (לדוגמה: רכיב מסכי המשתמש בענן אחד ורכיב BI ודוחות שיפעל בענן אחר) כשהשיקולים יהיו זמינות של שירותי Cloud Native מסויימים ופערים ביכולות של שירותים דומים המוצעים ע"י ספקיות ענן שונות.

11.5. הכפלה של מערכות ב-2 ספקי הענן

- זהו מקרה (נדיר יחסית) של הפעלה במקביל של רכיבים דומים בעננים של ספקיות שונות על מנת להבטיח זמינות, ביצועים (במקרה של מערכות תשתית המספקות שירות למערכות אחרות העשויות לפעול בכל אחת מספקיות הענן) וכדומה.
- ברוב המקרים אין צורך בהכפלה של הרכיבים בעננים של ספקיות שונות. ניתן לענות על הצורך בביצועים וביתירות של Data Centers גם כאשר בוחרים בספק ענן אחד (והאחריות לשרידות מתקני המחשב הינה על ספקית שירותי הענן).

11.6. תלות בספק שירותי ענן

- חשוב לזכור כי בסופו של דבר התלות בספק הענן הינה כמו התלות בכל ספק מוצר איסטרטגי אחר (בדומה לבחירה בספק של כלי פיתוח, מערכות-הפעלה או מוצר מדף).
- זכייתן של שתי ספקיות ענן במכרז נימבוס ענן מייצר ביטחון לגבי עצם קיום התחרות, התנאים לצריכת שירותים משתי ספקיות אלו ופשטות גבוהה יותר לבנות פתרונות המבוססים על רכיבים Cloud Native הזמינים על גבי הפלטפורמה של כל אחת מספקיות ענן אלו.

- הבחירה בספקית שירותי ענן הינה בחירה משולבת מקצועית/מסחרית עם שיקולים והעדפות ליכולות הפונקציונליות של השירותים המסופקים ע"י כל אחת מן הספקיות מול מדיניות התמחור של שירותים אלו – לצורך מתן המענה הנכון ביותר למימוש הדרישה העסקית.

12.חיבור וקישור רשתות

פרק זה הינו הנחייה כללית לעבודת המשרדים בענן, ללא קשר להחלטת המשרד לגבי יישום אזור הנחיתה (אם משרדי עצמאי או עבודה באזור הנחיתה הממשלתי).

12.1. **הפרדת סביבות ענן לפי סביבת הנתונים**[1]

- כדי לאפשר ניהול סיכונים בעבודה בענן ולאזן בינם לבין הדרישות הנובעות מהנחיות ושיקולי הגנת סייבר, במסגרת "איזורי נחיתה" המסופקים בתוך תשתית פלטפורמת ניהול הענן הממשלתית – ובהתאם לצורך, לדרישות וללוגיקה שתוגדר כחלק מתפיסת השירות והארכיטקטורה של הממשלה בענן – יוקצו מספר חשבונות עצמאיים לטובת כל משרד, ובמסגרתם יוגדרו עננים פרטיים וירטואליים שונים תוך הפרדה בין סביבות נתונים שונות.
- להלן הגדרת סוגי סביבות הנתונים לצורך סיווג ה- VPC-ים השונים, לפי סוג המידע המאוחסן בהם:
- סביבת PROD
  - VPC לצורך סביבות "גבוהות" (סביבות ייצור) – סביבות המכילות מידע אמת. גישה למשאבים בסביבה זו מחייב מירב הרגישות לכל היבטי אבטחת המידע וההגנה בסייבר. ב-VPC זה ניתן להגדיר גם רשתות ומשאבי ענן שאינם לצרכי ייצור, אך פועלים על עותק מלא של נתוני ייצור העדכניים לנקודת זמן כלשהי (נקרא לעיתים גם "צל-ייצור").
  - VPC לצורך סביבות "גבוהות לבדיקה " (סביבות Staging) – סביבות המכילות מידע אמת. גישה למשאבים בסביבה זו מחייב מירב הרגישות לכל היבטי אבטחת המידע וההגנה בסייבר. ב-VPC זה ניתן להגדיר גם רשתות ומשאבי ענן שאינם לצרכי ייצור, אך פועלים על עותק מלא של נתוני ייצור העדכניים לנקודת זמן כלשהי (נקרא לעיתים גם "צל-ייצור"). סביבה זו מיועדת להיות שלב לפני העברה לייצור לצורך בדיקות המערכת על מידע באופן מלא.
- סביבת NON-PROD
  - VPC לצורך סביבות "ביניים" (סביבות בדיקה) – סביבות המכילות מידע אמת חלקי ולפעמים משובש. גישה למשאבים בסביבות אלו מחייבת רגישות להיבטי הגנת הפרטיות וניהול סיכוני אבטחת מידע בהתאם לסוג ועומק המידע המאוחסן בהן.
  - VPC לצורך סביבות "נמוכות" (סביבות פיתוח) – סביבות המכילות רק מידע שאיננו אמת– מיועדות לצורך פיתוח ובדיקה. גישה למשאבים בסביבה זו אין בה סיכון לדליפת מידע.
- הסביבות מוגדרות להלן כ-"פיתוח, בדיקות וייצור". זאת, אף כי משרדים שונים יכולים לקבל החלטות שונות לגבי ה-VPC-ים בהם הם בוחרים לבצע את פעילויות מחזור חיי פיתוח התוכנה שלהם, בהתאם לנתונים הנתונים העומדים לרשותם בעבודה בענן. בהחלט ייתכן מצב בו יש הרבה יותר מ-3 חשבונות (או FOLDERS) לכל משרד והנושא הוא עניין למדיניות ספציפית שיגדיר כל משרד ומשרד.
- יש להדגיש כי קיימים ארגונים ממשלתיים רבים המבצעים גם כיום, בין אם מחוסר ברירה או כהחלטה מודעת, תחזוקה ו/או בדיקות בסביבות מידע המתאימות להגדרה להלן של "ייצור", או פיתוח בסביבות נתונים

[1] בהתאם למודל סיווג נתונים ומערכות

המתאימות להגדרה להלן של "בדיקות". בעבודה בענן חלוקה לסביבות עבודה מקבל חשיבות של ניהול, שרידות, גיבוי, הגנה בסייבר וניהול תקציבי בענן (FINOPS).

- הכלל לגבי קישור בין רשתות ומשאבי ענן המוגדרים ב- VPC-ים שונים (בין אם שייכים לחשבונות ומשרדים שונים ובין אם במסגרת אותו המשרד) הוא שניתן לקשר רק בין משאבים ורשתות בעלי אותו סוג סביבות נתונים.
- קישור והעברת נתונים בין רשתות ומשאבי ענן ב-VPC-ים השייכים לסביבות נתונים שונות יתבצע רק במסגרת הגדרת PIPELINE של ניהול מחזור חיי תוכנה באופן מאובטח (DEVSECOPS CI/CD), אשר יוגדר כחלק מנוהל פיתוח מאובטח בענן במסגרת תהליכי ה- DEVSECOPS של כל משרד ומשרד. חיבור כזה יתקיים בין VPC-ים שונים השייכים לאותו החשבון (=אותו המשרד) בלבד ויחייב אישור אבטחת מידע בהתאם להנחיות יה"ב המתאימות.

12.2. בידול רשתות וקישור רשתות בעלות רמת רגישות דומה ושונה

- בעת החיבור של רשתות עננים פרטיים וירטואליים יש להקפיד על הכלל של הפרדת VPC-ים בעלי סביבות נתונים שונות ועל כל כללי בידול הרשתות והנחיות אבטחת המידע המתייחסות לפתרונות מאובטחים לחיבור וקישור רשתות בעלות סוג סיווג מידע דומה ופתרונות להפרדה ובידול רשתות בעלות סוג סיווג מידע שונה.
- יש לזכור שהעובדה שהפתרון פועל "בענן" אין משמעותה שלא ניתן לאחסן בו מידע מסווג כלשהו, תחת הנחיות הבידול המתאימות, וכמו-כן, אין משמעות הדבר שהוא נגיש מהאינטרנט או על גבי האינטרנט. יש לקרוא בעיון את ההנחיות הישימות בנושא זה (הנחיות יה"ב או רשות הסייבר) וכל ה- BEST PRACTICE המקובלים בתחום.

13.תשתית MIDDLEWARE לעבודה היברידית

- על המשרד לתכנן כחלק מן "הגל הראשון" של המעבר לענן את התקנת מערכות התשתית היישומית (אפליקטיבית) המתווכת בין יישומים (ועל-כן מכונה "תווכה" - MIDDLEWARE) על מנת להבטיח עבודה ב-MULTI-CLOUD ועבודה היברידית (CLOUD + ON-PREM). ישנן מערכות רבות מסוג זה הפועלות כיום כחלק מן מתשתיות התוכנה במשרדי הממשלה אך הן לא הכרח מותאמות לעבודה בענן.
- כדי לאפשר עבודה היברידית (עבודה במקביל עם תשתיות הפועלות ב- DATA CENTER בחצרי הממשלה ועם תשתיות הפועלות בענן) – על המשרד לבחון שימוש בתשתיות MIDDLEWARE ייעודיות אשר מסוגלות להבטיח את האתגרים השונים הכרובים בעבודה היברידית בענן. לרוב נדרש לבחור מוצר או שירות שנועד מראש לעבודה בענן (CLOUD NATIVE) על מנת להבטיח התמודדות טובה יותר עם אתגרי תשתיות MIDDLEWARE בענן.
- שימוש בתשתיות MIDDLEWARE כ- IAAS: חלק מהמוצרים הקיימים בשוק מאפשרים פתרונות אבטחת מידע והבטחת רמת שירות (QUALITY OF SERVICE) טובים יותר מאחרים. במקרה זה תחזוקת המוצר, תצורתו, הסקלביליות שלו והבטחת רמת השירות שלו – הינם באחריות המשרד.
- שימוש בתשתיות MIDDLEWARE כ- PAAS: מודל מתקדם יותר המאפשר שימוש בפתרונות מבוססי API. כדי לחבר בין תשתית MIDDLEWARE הפועלת בחוות השרתים המשרדית לשירות הפועל כ- PAAS בענן נדרש לרוב סוג של CONNECTOR או GATEWAY (תלוי בפתרון).
- ניתן להשתמש בפתרונות PAAS MIDDLEWARE כאלו כ- SHARED SERVICE ממשלתי (תלוי באופי המידע המועבר ובסיווג הנתונים, ניתוח איומים, ניהול סיכונים ואבט"מ).
- ניתן להקים אותם כחלק מתצורת הרשת של ענן פרטי וירטואלי של המשרד בענן, וזאת – בין אם מדובר ברשת VPC במסגרת איזור נחיתה עצמאי המופעל ע"י המשרד בחשבון משלו, או ברשת VPC כזו המסופקת ע"י מערך הדיגיטל הלאומי בפלטפורמת ניהול הענן הממשלתי.

- סוג נוסף של תשתיות Middleware, המציע מודל ייחודי לעולם הענן, מבוסס על מודל ופתרונות API-as-a-Service. פתרונות אלו הם סוג של שירותי SaaS והם אינם מותקנים על גבי "איזור הנחיתה" בענן ולא במסגרת אחד השרתים המשמשים אותו (מלבד Gateway או Connector מקומי שתפקידו להעביר את המסרים ליעדם דרך הענן). תחזוקת המוצר, תצורתו, הסקלביליות שלו והבטחת רמת השירות שלו – הינם באחריות ספק שירותי הענן.
- אחד היתרונות החשובים של פתרונות מסוג זה הוא חסכון בהיבטי משאבי מחשוב וסקלביליות בלתי מוגבלת של הפתרון, תוך כדי תשלום רק לפי המשאבים בהם נעשה שימוש.
- יש לבחון את נושא הבטחת הפרטיות ושיקולי אבטחת מידע וסיווגו, כאשר משתמשים בפתרונות API-as-Service במודל SaaS.
- בדומה לשירותי Middleware כשירות בתצורת SaaS, קיימים גם שירותי DB-as-Service בענן המוצעים במודל SaaS. השיקולים לעבודה עם שירותים אלו דומים לאלו שתוארו בהקשר של Middleware-as-a-service, אולם שימוש בהם יהיה נדיר יותר בתצורה של ענן היברידי בשל שיקולי רמת שירות (תופעת ה- Latency וה- Delay הצפוי).
- בשימוש בשירותי Middleware בעבודה היברידית, יש לבצע ניתוח מדוקדק של רמת השירות הנדרשת, ה- Capacity המתוכנן, רמת האלסטיות של המשאבים הנדרשים כדי לתת לו מענה, וכן ה- Latency אותו יכולה המערכת לספוג.

14.פיתוח בענן

- אחד היתרונות החשובים הגלומים במעבר לעבודה בענן הוא היכולת להשתמש בכלי פיתוח מתקדמים ולהטמיע יחסית בקלות תהליכי הנדסת תוכנה, ניהול תצורה, אינטגרציה, פריסה ואוטומציה מתקדמים (DevOps).
- היתרון הגדול בשימוש בכלים אלו הוא הפוטנציאל הגבוה לשיתוף קוד וביצוע של פיתוחים רוחביים ופיתוחים המאפשרים שילוב מאמצים בין מספר משרדים ומספר גופים (בין שממשלתיים או אף חיצוניים לממשלה), וכל זאת ללא התפשרות על אבטחת מידע ועמידה בכללי הרגולציה השונים.
- השימוש בכלים אלו מבטיח סטנדרטיזציה, חיסכון בעלויות וקיצור זמני פיתוח, כמו גם עבודה אג'ילית יותר כתוצאה מקיצור משכי הזמן של מחזורי פיתוח ותחזוקה (משך הזמן שלוקח להוציא גרסה או תיקון מרגע ייזום שינוי ועד להפעלתו בייצור).
- הפיתוח בענן ישמש את ממשלת ישראל להתייעלות בפיתוח מערכות המשתפות מספר משרדי ממשלה, בפיתוחים רוחביים, בשיתוף קוד ויאפשר חסכון רב בתחזוקה ובשיפורים.
- כלים רבים מוצעים ע"י ספקי הענן אשר ניתן להשתמש בהם לפיתוח בענן. במסגרת רובד 5 במכרז נימבוס יתאפשר שימוש בכלים רבים נוספים המוצעים ע"י ספקי פתרונות צד ג' בענן. במסגרת מסמך תפעול הענן של ה- CCoE יפורט בהרחבה לגבי עולמות הפיתוח בענן וסוגי הכלים המשמשים לכך.
- ניתן להשתמש בשירותי ספקים במכרז הדיגיטל-טק להטמעת שימוש בכלים ובפתרונות CI/CD (Continuous Integration / Continuous Deployment) במסגרת עבודת המשרדים ובפרויקטים שלהם בשוטף ובעת מעבר לעבודה בענן.
- כלים המותקנים ופועלים בענן חוסכים מורכבויות של התקנה, קונפיגורציה ותחזוקה בצוותי המשרדים, ומקנים גמישות רבה יותר בשימוש בכלים. פיתוח כזה יכול להתבצע מכל מקום ללא תלות במיקום פיזי, בעמדת הפיתוח ותצורתה, ומאפשר גם עבודה מרחוק של צוותי פיתוח באופן מאובטח.
- יתרון נוסף של השימוש בכלי הפיתוח הזמינים בענן הוא שהם מוצעים כשירות, ומשכך, ניתן להטמיע בקלות את אבטחת המידע שרשרת הפיתוח בענן: DevSecOps. תהליכי השרשרת בפיתוח (Toolchains) המוצעים כשירות בענן יכולים לכלול בתצורה המוצעת לשירות משרדי ממשלה אספקטים שונים של פיתוח מאובטח וכלי

אבטחת מידע חיוניים, באופן שיבטיח עמידה בהנחיות יה"ב, מערך הסייבר ו ה- Best Practice המקובלים בתחום.

15.שימוש בקוד להקמה וניהול מערכות בענן

- את תצורת התשתיות בענן ניתן ליישם באמצעות מסכי קונפיגורציה אשר מעמידים ספקי הענן לרשות אנשי תשתיות ענן מומחים בתחומם.
- שיטה נוספת היא לעשות שימוש נרחב בקוד (Infrastructure as Code – IaC), ב- API של ספקי שירותי הענן, בקבצי קונפיגורציה (פורמטים שונים של JSON ו-XML) ובסקריפטים שונים (Terraforms, bash, PowerShell וכו') הפונים ל- API אלו ומשתמשים בקבצי הקונפיגורציה, כדי ליישם את הקמת תצורת הענן ולבצע את התחזוקה שלו ברמה גבוהה של אוטומציה וניהול גרסאות (כולל יכולת שחזור והתאוששות מתקלות).
- המדיניות הממשלתית להקמת תשתיות בענן תהיה לבצע זאת באמצעות קוד (IaC), ולא באמצעיים ידניים ,ע"י אנשי תשתיות ענן מומחים בתחומם. הגדרה באמצעות קוד יכולה לכלול גם סדרת הגדרות בסיסיות במערכת הניהול, הוספה של סקריפט הפועל באמצעות API או קובץ, או לטעון טמפלט ואז לשנות במסכי הניהול וכו'.
- גם הקמת משאבי ענן ע"י צוותי ה- DevOps המשרדיים בחשבונם בענן תתבצע ככל הניתן תוך שימוש ב- IaC (Infrastructure as Code).
- כאשר תצורת הענן מבוססת על קוד – תחזוקת הענן מאפשרת שיתוף שימוש חוזר ומתבססת על תשתית תוכנה וכלים לניהול קונפיגורציה ברמת אוטומציה גבוהה מאוד (DevOps). ניהול קוד זה במאגר מרכזי מאפשר למשרדים לשתף ביניהם ידע, יכולות, והגנות בסייבר, מסייעת במצמצום טעויות אנוש ומאפשרת שינויים בתשתיות (ניהול גרסאות). מאגר זה יוקם במערך הדיגיטל הלאומי באמצעות גוף ה- CCoE ויאפשר שיתוף קוד וידע בין משרדי הממשלה.
- הקמת תשתיות תוך שימוש בקוד מהווה קפיצת מדרגה ביכולות הטכנולוגיות העומדות לרשות המשרדים, ומבחינת יכולתה של הממשלה להגביר משילות, להחיל ולהטמיע הנחיות מדיניות באופן יעיל, גורף ורחב (ע"י פרסום מדיניות בקוד תוכנה, מה שנקרא "קבצי Policies" – Policy Files להלן) והטמעה שלו ע"י המשרדים השונים ולעדכן במהירות בכדי להגיב לשינויים הנדרשים.
- בהקמת תשתיות ענן בשיטה זו מתקבלת סביבה מאובטחת, מבוקרת ומתועדת, אשר ניתן להרחיבה בזמני תגובה חסרי תקדים בהשוואה לזמן הנדרש להקמת תשתיות פיזיות ב- Data Center מקומי (החל מרכש וכלה בהתקנה, הפעלה והקשחה כנדרש) וגם ביחס להקמה של תשתית ענן באופן ידני.

16.מסמכים ישימים וקשורים

- הנחיית CCoE להיערכות למעבר לענן
- מדיניות ממשלתית להגנת סייבר בענן ציבורי (מסמך זה זמין לממונה ההגנה בסייבר המשרדי)

17.נספחים

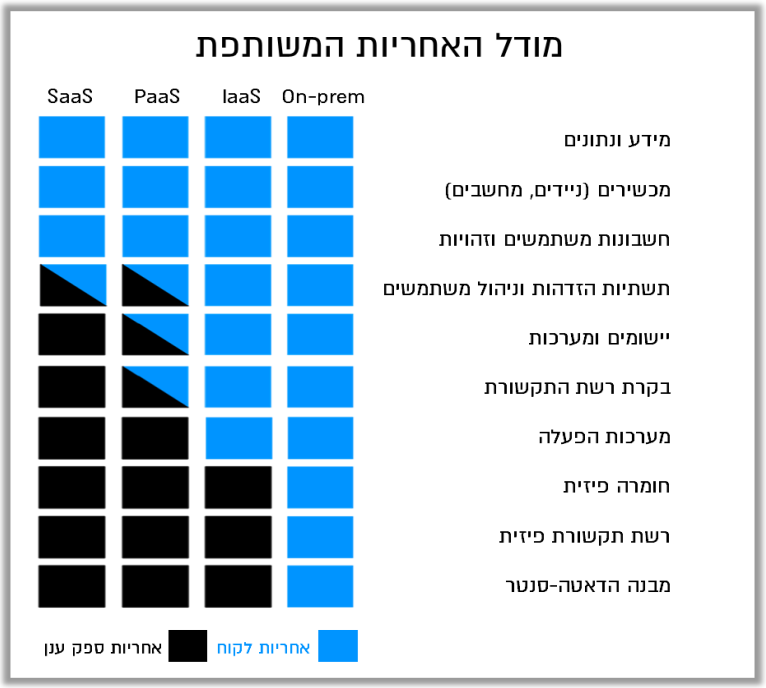
מיגרציה לענן

כחלק מן "המסע לענן" בממשלה אשר מנוהג ע"י פרויקט נימבוס, פותחה הנחיית CCoE להיערכות למעבר לענן ומתואמת עם מסמך אסרטגיית הענן הממשלתית. ההנחיה מיועדת להתפתח ולהתרחב באופן מתמיד במסגרת גרסאות עתידיות וזאת על בסיס משוב עתידי מן השטח ובקשות של המשתמשים/לקוחות.

מעבר לזה, היא מיועדת לשמש מעין מתווה קונספטואלי למשרדים, אשר יכול לשמש כקלט לפעילויות המעבר לענן ולענות על שאלות אשר עולות במהלך תוכניות מעבר לענן. במסגרת הנחיית CCoE למעבר לענן מופיעים עקרונות מנחים מפורטים לנושאים אלו.

מודל האחריות המשותפת של ספק ענן

ספק שירותי הענן אחראי לספק רכיבים מסויימים של הפתרון, לדאוג לאבטחת המידע הבסיסית של מתקן המחשב ולהעמדת פתרונות אבטחת מידע לשימוש ביישום רכיבי הפתרון המסופקים ע"י הלקוח (כלומר, המשרד הממשלתי), בהם ניתן לעשות שימוש כפי הצורך. השימוש בהם והיישום שלהם כדי להבטיח עמידה בדרישות אבטחת המידע הינו באחריות המשרד. שכבות הפתרון אותן מספק הלקוח ועליהן נדרש המשרד להגן תלויות בסוג שירותי הענן המהווים חלק מן הפתרון.



18.גרסאות ההנחיה

מס'	סטאטוס	מהות שינוי	סעיפים שהושפעו	בתוקף מ-	נכתב ע"י	אושר ע"י
0.1	טיוטה להתייחסות	טיוטה להתייחסות		01.12.2022	קרן בר-לב	טיוטה להתייחסות